SonicWALL Global Management System Reporting User Guide

Version 2.5

Copyright Information

© 2003 SonicWALL, Inc. All rights reserved.

Under the copyright laws, this manual or the software described within, may not be copied, in whole or part, without the written consent of the manufacturer, except in the normal use of the software to make a backup copy. The same proprietary and copyright notices must be affixed to any permitted copies as were affixed to the original. Under the law, copying includes translating into another language or format.

SonicWALL is a registered trademark of SonicWALL, Inc.

Other product and company names mentioned herein may be trademarks and/or registered trademarks of their respective companies.

Specifications and descriptions subject to change without notice.

Part Number: 232-000187-01 Rev A

Software License Agreement for SonicWALL Global Management System

To review the SonicWALL Global Management System Software License Agreement, see the *SonicWALL Global Management System Introduction Guide*.

Chapter 1 Introducing ViewPoint Reporting **7**

Chapter 2 Configuring GMS Reporting Settings **9**
Enabling GMS Reporting **10**
Configuring the Syslog Event Rate **11**
Configuring GMS Reporting Module Settings **12**
Distributed Scheduler **12**
General Report Settings **12**
Configuring Log Viewer Settings **13**
Configuring Email/Archive Settings **14**

Chapter 3 Viewing Reports **17**
Viewing Bandwidth Reports **17**
Viewing the Bandwidth Summary Report **17**
Monitoring Bandwidth Usage in Real Time **19**
Viewing the Top Users of Bandwidth **19**
Viewing Bandwidth Usage Over Time **21**
Viewing the Top Users of Bandwidth Over Time **22**
Viewing Service Usage Reports **24**
Monitoring Service Usage in Real Time **24**
Viewing the Services Summary Report **25**
Adding a Service **26**
Viewing Web Usage Reports **27**
Viewing the Web Usage Summary Report **27**
Viewing the Top Sites **29**
Viewing the Top Users of HTTP Bandwidth **30**
Viewing HTTP Bandwidth Usage by User **32**
Viewing Bandwidth Usage Over Time **33**
Viewing Top Sites Over Time **34**
Viewing Top Users Over Time **35**
Viewing Bandwidth Usage By User Over Time **37**
Viewing Web Filter Reports **39**
Viewing the Web Filter Summary Report **39**
Viewing the Web Filter Top Sites Report **40**
Viewing the Top Users that Try to Access Blocked Sites **42**
Viewing the Top Blocked Sites for Each User **43**
Viewing Blocked Site Attempts Over Time **45**
Viewing the Top Blocked Site Attempts Over Time **46**
Viewing the Top Blocked Site Users Over Time **47**
Viewing the Top Blocked Sites for Each User Over Time **49**
Viewing File Transfer Protocol Reports **51**
Viewing the FTP Summary Report **51**
Viewing the Top Users of FTP Bandwidth **52**
Viewing FTP Bandwidth Usage Over Time **54**
Viewing the Top Users of FTP Bandwidth Over Time **55**

Viewing Mail Usage Reports **57**
Viewing the Mail Usage Summary Report **57**
Viewing the Top Users of Mail Bandwidth **59**
Viewing Mail Usage Over Time **60**
Viewing the Top Users of Mail Bandwidth Over Time **62**
Viewing VPN Usage Reports **64**
Viewing the VPN Usage Summary Report **64**
Viewing the Top VPN Users **65**
Viewing VPN Usage Over Time **67**
Viewing the Top VPN Users Over Time **68**
Viewing Attack Reports **70**
Viewing the Attack Summary Report **70**
Viewing the Attacks by Category **71**
Viewing the Attacks by Source **73**
Viewing the Errors and Exceptions Report **74**
Viewing Attack Reports Over Time **76**
Viewing Errors Over Time **77**
Categories Over Time **78**
Sources Over Time **80**
Viewing Authentication Reports **82**
Viewing the User Login Report **82**
Viewing the Administrator Login Report **83**
Viewing the Failed Login Report **84**
Viewing the Log **86**
Viewing the Log for a SonicWALL Appliance **86**
Viewing the Log for a Ravlin Device **87**

Chapter 4 Scheduling GMS Reporting **91**
Scheduling a Daily Report **92**
Scheduling a Weekly or Monthly Report **93**

Chapter 5 Customizing Report Elements **97**
Using the Reporting Customization Tool **98**
Scheduling a Report **98**
Firmware 6.5 **101**
SonicOS 1.0 **111**

Introducing ViewPoint Reporting

Monitoring critical network events and activity, such as security threats, inappropriate Web use, and bandwidth levels, is an essential component of network security. GMS Reporting complements SonicWALL's Internet security offerings by providing detailed and comprehensive reports of network activity.

The GMS Reporting Module is a software application that creates dynamic, Web-based network reports. The GMS Reporting Module generates both real-time and historical reports to offer a complete view of all activity through SonicWALL Internet security appliances. With GMS Reporting, you can monitor network access, enhance security, and anticipate future bandwidth needs.

The GMS Reporting Module:

- Displays bandwidth use by IP address and service
- Identifies inappropriate Web use
- Provides detailed reports of attacks
- Collects and aggregates system and network errors
- Shows VPN events and problems
- Presents visitor traffic to your Web site
- Provides detailed daily firewall logs to analyze specific events.

Note: *The GMS Reporting Module receives its information from the stream of syslog data sent by each SonicWALL appliance and stores it in the ViewPoint database.*
GMS Reporting can be enabled or disabled. Once disabled, the Reports tab disappears from the ViewPoint User Interface (UI) and the syslog data is no longer stored.

Note: *For Ravlin devices, GMS Reporting provides detailed firewall logs to analyze specific events. It does not provide real-time and historical Web-based network reporting.*

Configuring GMS Reporting Settings

This chapter describes how to enable or disable the GMS Reporting Module, configure the syslog event rate, and configure GMS Reporting settings. Select from the following:

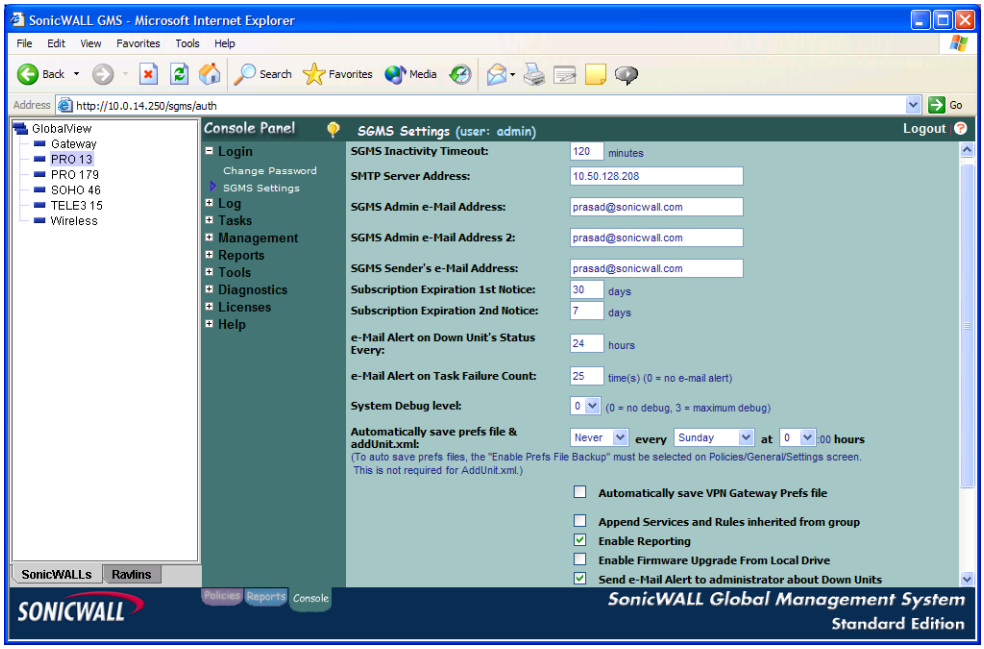
- To enable or disable the GMS Reporting Module, see “Enabling GMS Reporting” on page 10.
- To configure the syslog event rate to accurately report all firewall information, see “Configuring the Syslog Event Rate” on page 11.
- To configure GMS Reporting settings, see “Configuring GMS Reporting Module Settings” on page 12.

Enabling GMS Reporting

By default, GMS Reporting is enabled. To enable or disable GMS Reporting, follow these steps:

1. Start and log into ViewPoint.
2. Click the **Console Panel** tab at the bottom of the ViewPoint UI.
3. Expand the Login tree and click **SGMS Settings**. The SGMS Settings page appears (Figure 1).

Figure 1: SGMS Settings Page



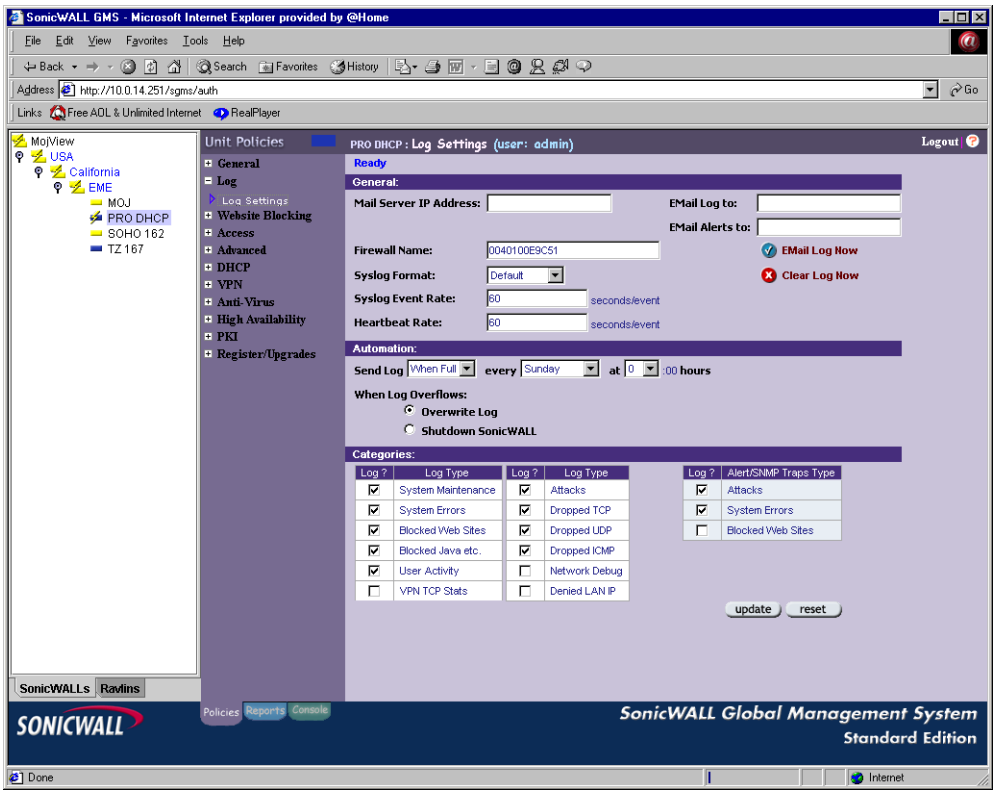
4. To enable GMS Reporting, select the **Enable Reporting** check box. To disable it, deselect the **Enable Reporting** check box (default: Enabled).
5. When you are finished, click **Update**.

Configuring the Syslog Event Rate

To configure the syslog event rate, follow these steps:

1. Start and log into ViewPoint.
2. Click the **Policies** tab.
3. Select the global icon, a group, or a SonicWALL appliance.
4. Expand the Log tree and click **Log Settings**. The Log Settings page appears (Figure 2).

Figure 2: Log Settings Page



5. Enter 0 in the **Syslog Event Rate** field.

   The Syslog Event Rate field reduces the number of repetitive events that are logged by ViewPoint. Although this prevents a log file from being full of repetitive events, setting the Syslog Event Rate field to anything other than 0 will result in inaccurate reporting.

6. To make sure that the GMS Reporting Module can display all reports, make sure that every event category in the Categories area is selected except for Network Debug.
7. When you are finished, click **Update**. The Syslog Event Rate is changed and every event category is enabled for each selected SonicWALL appliance.

Configuring GMS Reporting Module Settings

This section describes how to configure reporting settings. These include how often the summary information is updated, the number of days that summary information is stored, and the number of days that raw data is stored.

These reports are constructed from the most current available summary data. In order to create summary data, the GMS Reporting Module must parse the raw data files.

Note: *Because reports are based on the most current summary data, the report may be old. For example, if the data was summarized four hours ago, all activity that occurred since the last summary will be missing from the report.*

When configuring GMS Reporting, you can select the amount of summary information to store. Summary information consumes approximately one kilobyte of information per SonicWALL appliance per day. Make sure the database is large enough to accommodate the number of days that you choose.

Additionally, you can select the amount of raw data to store. The raw data is made up of information for every connection. Depending on the amount of traffic, this can quickly consume an enormous amount of space in the database. Be very careful when selecting how much raw information to store.

Distributed Scheduler

The Distributed Scheduler provides improved performance over the old Scheduler. The following describes the processing and summarization process of the Distributed scheduler:

- As incoming events are sent to the Agent, they are written to a file in the <*sgms_directory*>/logs directory. The format of the file is:

  *agentid_start-date_start-time*_**to**_*end-date_end-time*.**unp**

  where *agentid* is the ID of the agent, *start-date* is the starting date (YYYYDD), *start-time* is the starting time (HHMMSS), *end-date* is the ending date, and *end-time* is the ending time.
- When the file contains 10,000 lines, the Distributed Scheduler closes the file and begins creating a new one.
- At the interval you specify, the Distributed Scheduler changes the extension of the file to .prg and begins processing the file and storing its information as summarized data. It repeats this process for every file ending with the extension .unp.
- After it processes a file, it changes its extension to .PRD.

If you choose to use the Distributed Scheduler, you will need to periodically delete files with the .PRD extension to prevent your disk from filling. Additionally, the Distributed Scheduler does not store raw data, so no information will appear in the log viewer.

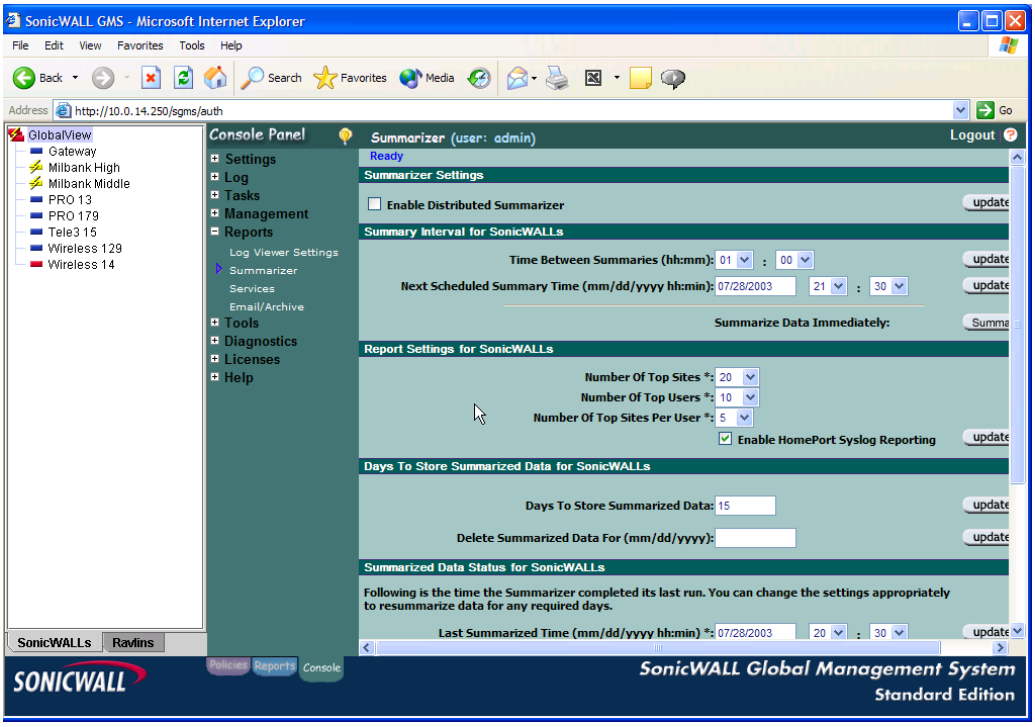
General Report Settings

Periodically, the SonicWALL appliances send their syslog files to the Agent. At the interval you specify, the Agent's Summarizer will process those files and store the data in the raw and summary databases.

To configure Summarizer settings, follow these steps:

1. Start and log into ViewPoint.
2. Click the **Console** tab.
3. Select a SonicWALL appliance.
4. Expand the Reports tree and click **Summarizer**. The Summarizer page appears (Figure 3).

Figure 3: Summarizer Page



5. Previous generations of the Summarizer wrote raw data directly to the database and periodically parsed it and stored it as summarized data. This is very resource-intensive. The Distributed Summarizer writes events to directly to log files which it parses periodically and stores as summarized data.

   To improve performance, select the **Enable Distributed Summarizer** check box. However, keep in mind that you will not be able to view individual events in the Log Viewer and you will periodically need to open the log file directory and delete old events. Otherwise, it can begin to consume significant amounts of space.

6. Specify how often the GMS Reporting Module processes and updates summary information from the **Time Between Summaries** list box and click **Update**.

7. To specify the next summary time, enter a date and time in the **Next Scheduled Summary Time** field and click **Update**.

8. To update the summary information now, click **Summarize Data Immediately**. ViewPoint will automatically process the latest information and make it available for immediate viewing.

   Note: *This will not affect the normally scheduled summarization updates.*

9. Configure the following report setting defaults:

   - Select the default number of sites that will be displayed in Top Sites reports from the **Number of Top Sites** list box (default: 10).
   - Select the default number of users that will be displayed in Top Users reports from the **Number of Top Users** list box (default: 10).
   - Select the default number of sites that will be displayed in Top Sites Per User reports from the **Number of Top Sites Per User** list box (default: 10).

10. Specify how many days of summarized data the GMS Reporting Module will store in the database from the **Days To Store Summarized Data** list box (default: 15) and click **Submit**. To save all information, enter **All**.

    Summarized data consumes approximately one kilobyte of information per SonicWALL appliance per day. Make sure the database is large enough to accommodate the number of days that you choose.

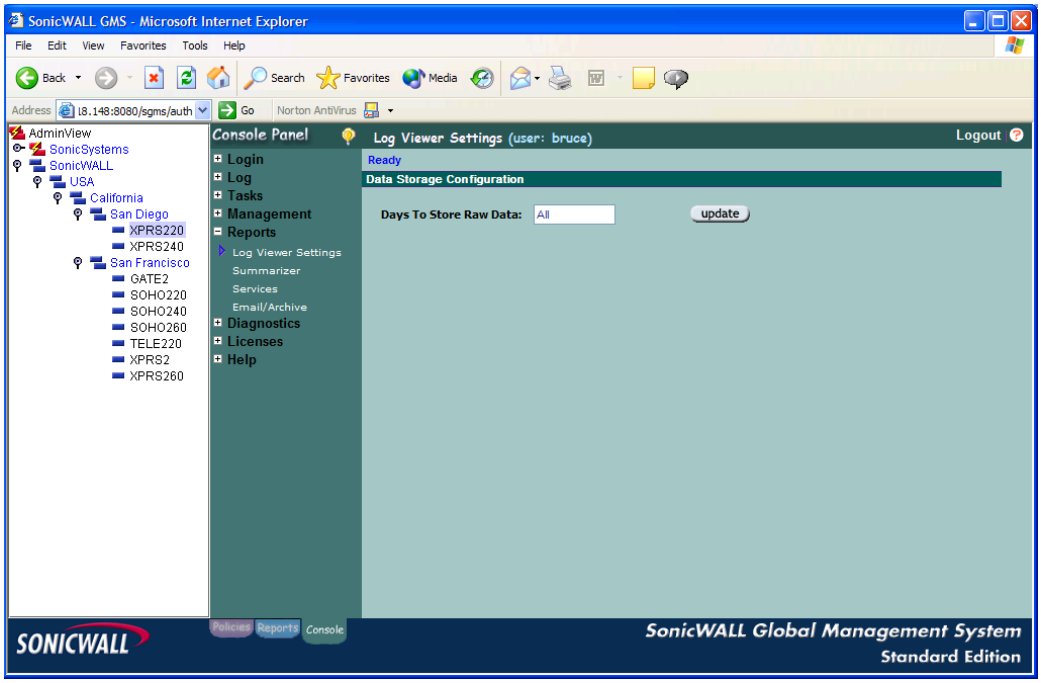
11. The **Summary Data Available Until** field displays when the data was last summarized. To re-summarize any data, enter a date and time and click **Update**.

Configuring Log Viewer Settings

To configure Log Viewer settings, follow these steps:

1. Start and log into ViewPoint.
2. Click the **Console** tab.
3. Select a SonicWALL appliance.
4. Expand the Reports tree and click **Log Viewer Settings**. The Log Viewer Settings page appears (Figure 4).

Figure 4: Log Viewer Settings Page



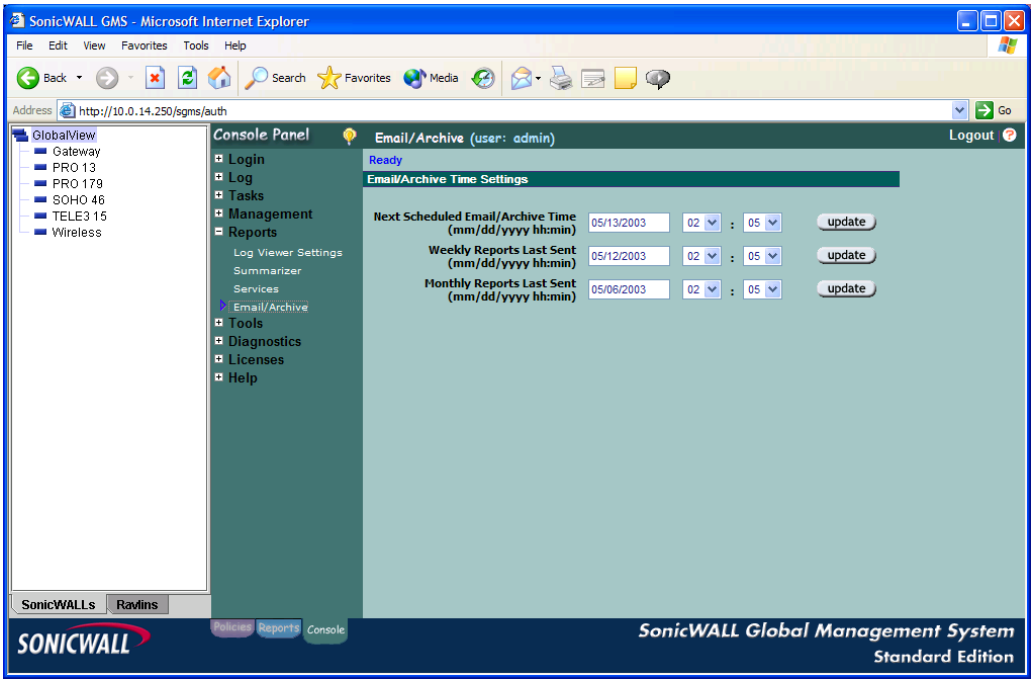
5. Specify how many days of raw data ViewPoint will store in the database from the **Days To Store Raw Data** list box and click **Submit**. To save all information, enter **All**.
6. To save the changes, click **Submit**.

Configuring Email/Archive Settings

To configure Email/Archive settings, follow these steps:

1. Start and log into ViewPoint.
2. Click the **Console** tab.
3. Select a SonicWALL appliance.
4. Expand the Reports tree and click **Email/Archive**. The Email/Archive page appears (Figure 5).

Figure 5: Log Viewer Settings Page



5. This page shows when the next scheduled archive time will occur and when the last weekly and monthly reports were sent.
6. To set the next archive time, enter the date and time in the **Next Scheduled Email/Archive Time** fields and click **Update**.
7. To specify when the next weekly report will be sent, enter the date and time in the **Weekly Reports Last Sent** fields and click **Update**.
8. To specify when the next monthly report will be sent, enter the date and time in the **Monthly Reports Last Sent** fields and click **Update**.

Viewing Reports

This chapter describes how to generate reports using Standalone ViewPoint (ViewPoint) Reporting Module.

Select from the following reports:

- To view general bandwidth usage reports, see "Viewing Bandwidth Reports" on page 17.
- To view bandwidth reports, by service, see "Viewing Service Usage Reports" on page 24.
- To view web usage bandwidth reports, see "Viewing Web Usage Reports" on page 27.
- To view reports on the number of attempts that users made to access blocked websites, see "Viewing Web Filter Reports" on page 39.
- To view file transfer protocol (FTP) bandwidth usage reports, see "Viewing File Transfer Protocol Reports" on page 51.
- To view mail bandwidth usage reports, see "Viewing Mail Usage Reports" on page 57.
- To view virtual private networking (VPN) reports, see "Viewing VPN Usage Reports" on page 64.
- To view reports on attempted attacks, see "Viewing Attack Reports" on page 70.
- To view detailed logging information, see "Viewing the Log" on page 86.
- To view user and administrator authentication reports, see "Viewing Authentication Reports" on page 82.

Viewing Bandwidth Reports

Bandwidth reports display the amount of data transferred through the selected SonicWALL appliance(s).

Bandwidth reports are an ideal starting point for viewing overall bandwidth usage. You can view bandwidth usage view by the hour, day, or over a period of days. Additionally, you can view the top users of bandwidth.

From this information, you can determine network strategies. For example, if you need more bandwidth, you might need to upgrade network equipment, or you might simply need to curtail the bandwidth usage of a few employees.

Note: *All reports appear in Universal Time, Coordinated (UTC) or Greenwich Mean Time (GMT).*

Select from the following:

- To view a summary of the daily bandwidth usage, see "Viewing the Bandwidth Summary Report" on page 17.
- To view bandwidth usage in real time, see "Monitoring Bandwidth Usage in Real Time" on page 19.
- To view the users who consume the most bandwidth, see "Viewing the Top Users of Bandwidth" on page 19.
- To view bandwidth usage over a period of time, see "Viewing Bandwidth Usage Over Time" on page 21.
- To view the users who consume the most bandwidth over time, see "Viewing the Top Users of Bandwidth Over Time" on page 22.

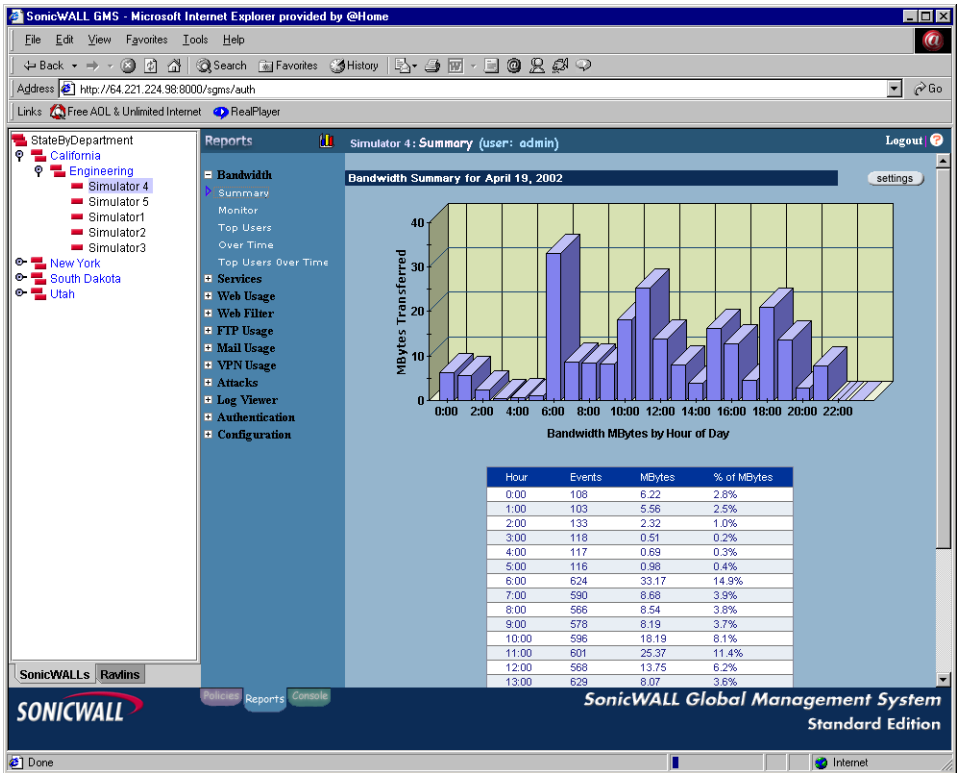
Viewing the Bandwidth Summary Report

The Bandwidth Summary report contains information on the amount of traffic handled by a SonicWALL appliance or group of SonicWALL appliances during each hour of the specified day.

To view the Bandwidth Summary report, follow these steps:

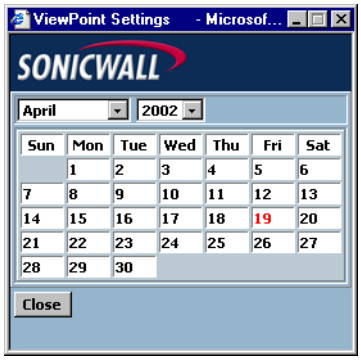
1. Start and log into ViewPoint.
2. Click the **Reports** tab.
3. Select the global icon, a group, or a SonicWALL appliance.
4. Expand the Bandwidth tree and click **Summary**. The Summary page appears (Figure 6).

Figure 6: Summary Page



5. The bar graph displays the amount of bandwidth transferred during each hour of the day.
6. The table contains the following information:
   - **Hour**—when the sample was taken.
   - **Events**—number of events or "hits."
   - **MBytes**—number of megabytes transferred.
   - **% of MBytes**—percentage of megabytes transferred during this hour, compared to the day. For example, if 1000 megabytes of data was transferred during the day and 100 megabytes was transferred at the 12:00 time period, the **% of MBytes** field will display 10%.
7. The GMS Reporting Module shows today's report. To change the date of the report, click **Settings**. The Report Settings dialog box appears (Figure 7).

Figure 7: Report Settings Dialog Box


ViewPoint Settings - Microsof...
SONICWALL
April
2002
Sun Mon Tue Wed Thu Fri Sat
1 2 3 4 5 6
7 8 9 10 11 12 13
14 15 16 17 18 19 20
21 22 23 24 25 26 27
28 29 30
Close

8. Select the year, month, and day that you would like to view.
9. When you are finished, click **Close**. The GMS Reporting Module displays the report for the selected day.

   Note: *These settings will stay in effect for all reports during your active login session.*

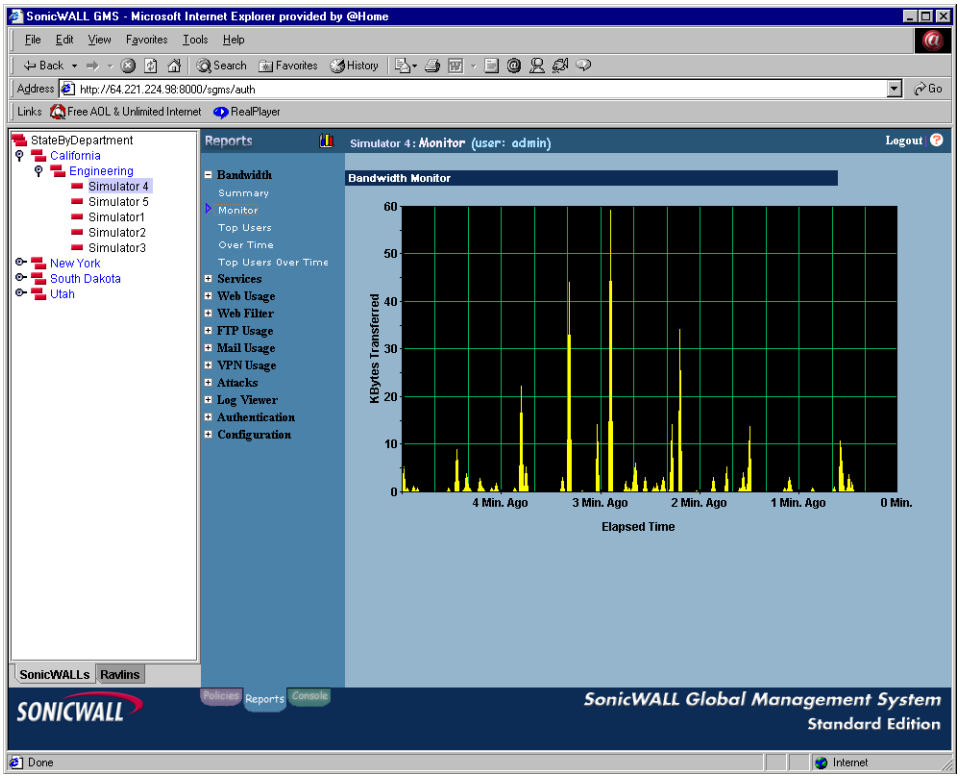
Monitoring Bandwidth Usage in Real Time

The Bandwidth Monitor displays bandwidth usage for the selected SonicWALL appliance in real time.

To view the Bandwidth Monitor, follow these steps:

1. Start and log into ViewPoint.
2. Click the **Reports** tab.
3. Select a SonicWALL appliance.
4. Expand the Bandwidth tree and click **Monitor**. The Monitor page appears (Figure 8).

Figure 8: Monitor Page



5. The Bandwidth Monitor shows the amount of data transferred during each sampling period for the last five minutes. The sampling period is five seconds.

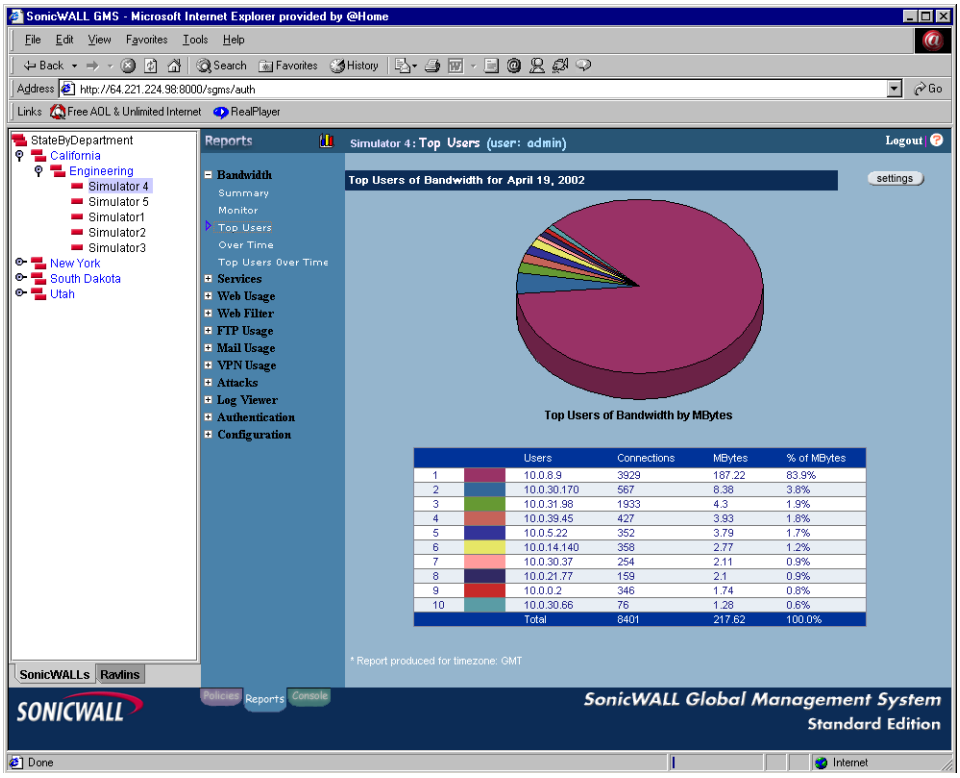
Viewing the Top Users of Bandwidth

The Top Users report displays the users who used the most bandwidth on the specified date.

To view the Top Users report, follow these steps:

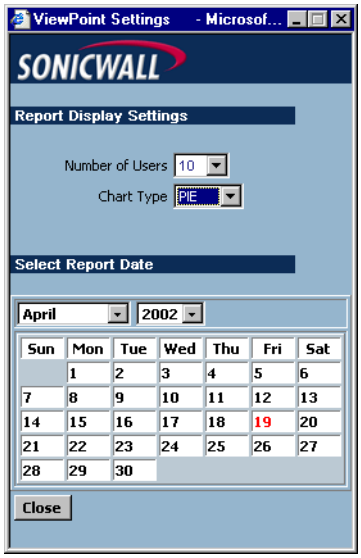
1. Start and log into ViewPoint.
2. Click the **Reports** tab.
3. Select a SonicWALL appliance.
4. Expand the Bandwidth tree and click **Top Users**. The Top Users page appears (Figure 9).

Figure 9: Top Users Page



5. The pie chart displays the percentage of bandwidth transferred by each user.
6. The table contains the following information:
   - **Users**—the IP address of the user.
   - **Connections**—number of events or "hits."
   - **MBytes**—number of megabytes.
   - **% of MBytes—**percentage of megabytes transferred by this user, compared to all users. For example, if 1000 megabytes of data was transferred during the day and 200 megabytes was transferred by the top user, the **% of MBytes** field will display 20%.
7. By default, the GMS Reporting Module shows today's report, a pie chart, and the ten top users. To change these settings, click **Settings**. The Report Settings dialog box appears.

Figure 10: Report Settings Dialog Box


ViewPoint Settings - Microsof...
SONICWALL
Report Display Settings
Number of Users 10
Chart Type PIE
Select Report Date
April 2002
Sun Mon Tue Wed Thu Fri Sat
1 2 3 4 5 6
7 8 9 10 11 12 13
14 15 16 17 18 19 20
21 22 23 24 25 26 27
28 29 30
Close

8. Select the number of users that will be displayed from the **Number of Users** list box.
9. Select the type of chart from the **Chart Type** list box.
10. Select the year, month, and day that you would like to view.
11. When you are finished, click **Close**. The GMS Reporting Module displays the report for the selected day.

    Note: *These settings will stay in effect for all reports during your active login session.*

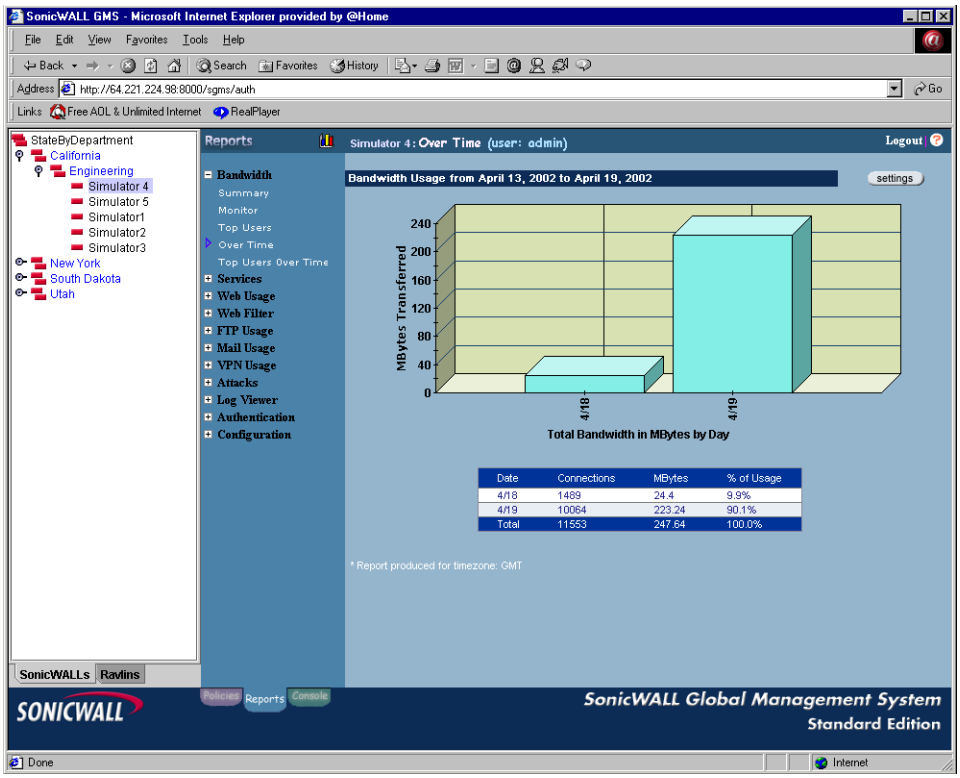
Viewing Bandwidth Usage Over Time

The Bandwidth Over Time report displays the daily amount of traffic handled by a SonicWALL appliance or a group of SonicWALL appliances for the specified time period.

To view the Bandwidth Over Time report, follow these steps:

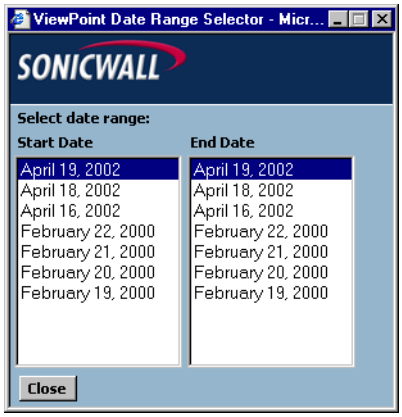
1. Start and log into ViewPoint.
2. Click the **Reports** tab.
3. Select the global icon, a group, or a SonicWALL appliance.
4. Expand the Bandwidth tree and click **Over Time**. The Over Time page appears (Figure 11).

Figure 11: Over Time Page



5. The bar graph displays the amount of bandwidth transferred during each day of the specified time period.
6. The table contains the following information:
   - **Date**—when the sample was taken.
   - **Connections**—number of hits.
   - **MBytes**—number of megabytes transferred.
   - **% of Usage**—percentage of megabytes transferred during this day, compared to the time period. For example, if 100,000 megabytes of data was transferred during the time period and 25,000 megabytes was transferred on one day, the **% of Usage** field will display 25%.
7. To change the date range of the report, click **Settings**. The Reporting Date Range Selector dialog box appears.

Figure 12: Report Settings Dialog Box



8. Select the starting and ending dates that you would like to view.
9. When you are finished, click **Close.** The GMS Reporting Module displays the report for the selected date range.

   Note: *These settings will stay in effect for all reports during your active login session.*

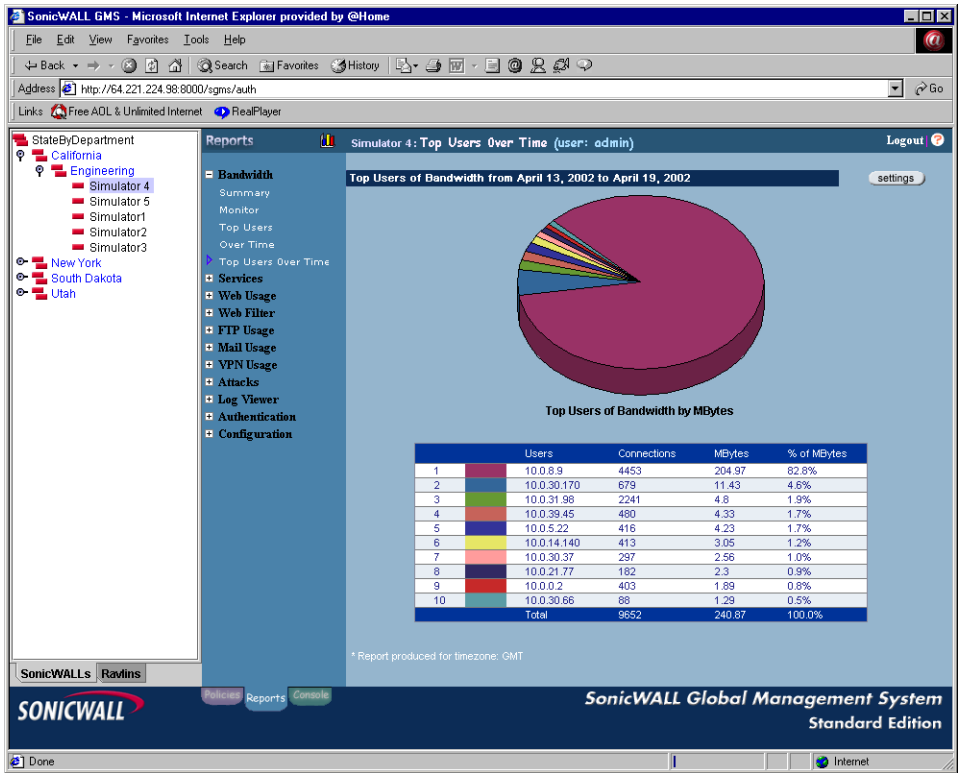
Viewing the Top Users of Bandwidth Over Time

The Top Users report displays the users who used the most bandwidth on the specified date.

To view the Top Users Over Time report, follow these steps:

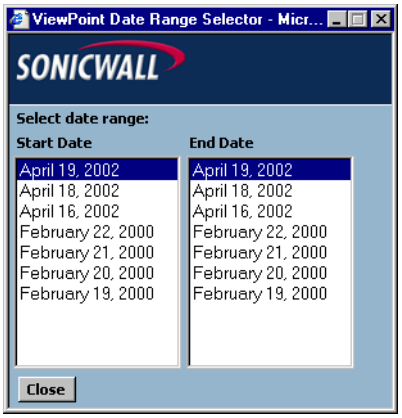
1. Start and log into ViewPoint.
2. Click the **Reports** tab.
3. Select a SonicWALL appliance.
4. Expand the Bandwidth tree and click **Top Users Over Time**. The Top Users Over Time page appears (Figure 13).

Figure 13: Top Users Over Time Page



5. The pie chart displays the percentage of bandwidth transferred by each user.
6. The table contains the following information:
   - **Users**—the IP address of the user.
   - **Connections**—number of events or "hits."
   - **MBytes**—number of megabytes.
   - **% of MBytes—**percentage of megabytes transferred by this user, compared to all users. For example, if 1000 megabytes of data was transferred during this period and 200 megabytes was transferred by the top user, the **% of MBytes** field will display 20%.
7. To change the date range of the report, click **Settings**. The Reporting Date Range Selector dialog box appears.

   Figure 14: Report Settings Dialog Box



8. Select the starting and ending dates that you would like to view.
9. When you are finished, click **Close.** The GMS Reporting Module displays the report for the selected date range.

   Note: *These settings will stay in effect for all reports during your active login session.*

Viewing Service Usage Reports

Service reports provide information on the amount of data transmitted through the selected SonicWALL appliance by each service.

Service reports are useful for revealing inappropriate usage of bandwidth and can help determine network policies. For example, if there is a large spike of bandwidth usage, you can determine whether this is caused by regular web access, someone using FTP to transfer large files, an attempted Denial of Service (DoS) attack, or another service.

Note: *All reports appear in Universal Time, Coordinated (UTC) or Greenwich Mean Time (GMT).*

The GMS Reporting Module can monitor known services as well as custom services. To add a service to monitor, see "Adding a Service" on page 26.

Select from the following:

- To view service bandwidth usage in real time, see "Monitoring Service Usage in Real Time" on page 24.
- To view a summary of the daily service bandwidth usage, see "Viewing the Services Summary Report" on page 25.

Note: *You cannot view services reports from the global or group view.*

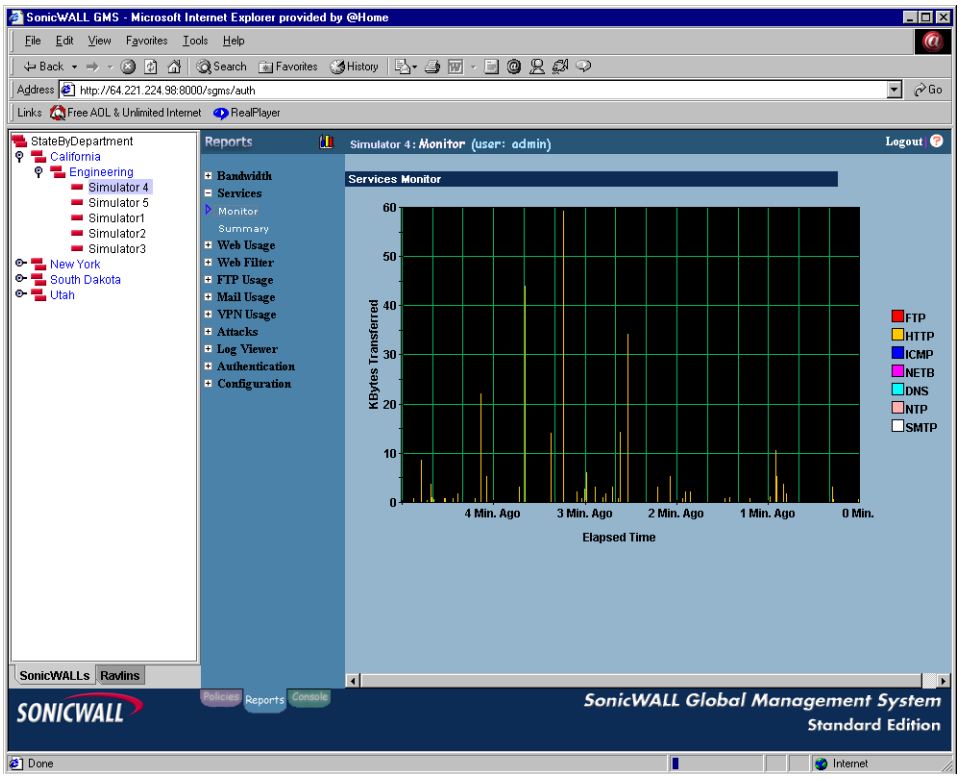
Monitoring Service Usage in Real Time

The Services Monitor displays service usage for the selected SonicWALL appliance in real time.

To view the Service Monitor, follow these steps:

1. Start and log into ViewPoint.
2. Click the **Reports** tab.
3. Select a SonicWALL appliance.
4. Expand the Services tree and click **Monitor**. The Monitor page appears (Figure 15).

Figure 15: Monitor Page



5. The Services Monitor shows the amount of data transferred for each service during each sampling period for the last five minutes. The sampling period is 15 seconds.

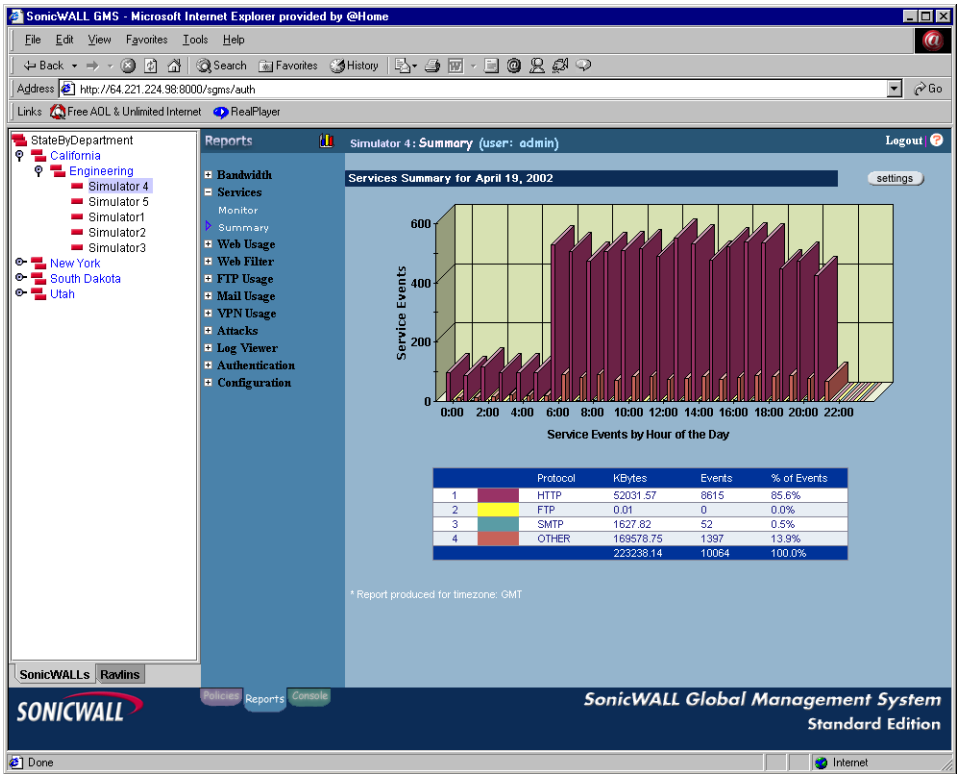
Viewing the Services Summary Report

The Services Summary report displays the amount of traffic handled by each service during each hour of the specified day.

To view the Services Summary report, follow these steps:

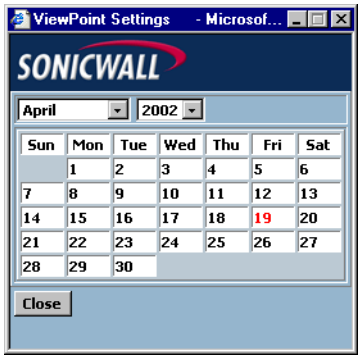
1. Start and log into ViewPoint.
2. Click the **Reports** tab.
3. Select a SonicWALL appliance.
4. Expand the Services tree and click **Summary**. The Summary page appears (Figure 16).

Figure 16: Summary Page



5. The bar graph displays the amount of bandwidth used by each service during each hour of the day.
6. The table contains the following information:
   - **Protocol**—the service.
   - **KBytes**—number of kilobytes.
   - **Events**—number of events or "hits."
   - **% of Events**—percentage of events transferred by this service on the selected day, compared to all other services. For example, if 10,000 events occurred during the day and 9,000 of the events were handled by the HTTP service, the **% of Events** field will display 90%.
7. The GMS Reporting Module shows today's report. To change the date of the report, click **Settings**. The Report Settings dialog box appears (Figure 17).

Figure 17: Report Settings Dialog Box


ViewPoint Settings - Microsof...
SONICWALL
April
2002
Sun Mon Tue Wed Thu Fri Sat
1 2 3 4 5 6
7 8 9 10 11 12 13
14 15 16 17 18 19 20
21 22 23 24 25 26 27
28 29 30
Close

8. Select the year, month, and day that you would like to view.
9. When you are finished, click **Close.** The GMS Reporting Module displays the report for the selected day.

   Note: *These settings will stay in effect for all reports during your active login session.*

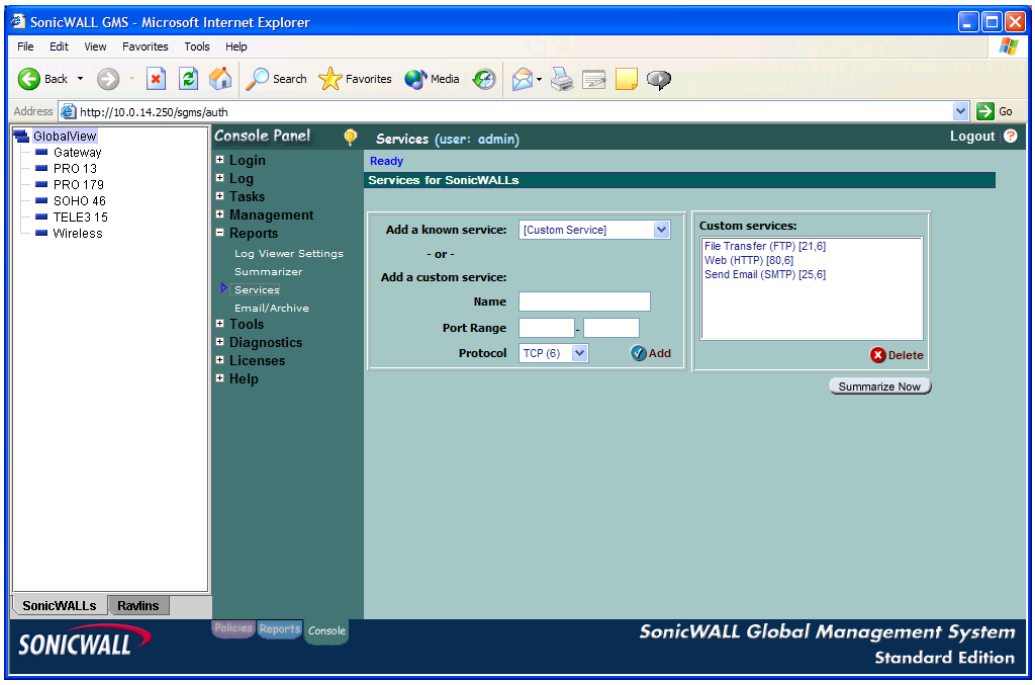
Adding a Service

The GMS Reporting Module can monitor known services or custom services.

To add a service that will be displayed in the services reports, follow these steps.

1. Start and log into ViewPoint.
2. Click the **Reports** tab.
3. Expand the Reports tree and click **Services**. The Services page appears (Figure 16).

Figure 18: Summary Page



4. To add a known service, select it from the **Known Services** list box and click **Add**.
5. To add a custom service, enter a name in the **Name** field, enter the service's port range, and select the protocol that it uses from the **Protocol** list box. Click **Add**.
6. To delete a service, select it and click **Delete**.

Viewing Web Usage Reports

Web usage reports provide information on the amount of web usage that occurs through the selected SonicWALL appliance(s).

Web usage reports can be used to view web bandwidth usage by the hour, day, or over a period of days. Additionally, you can view the top users of web bandwidth and view the most visited sites.

Note: *All reports appear in Universal Time, Coordinated (UTC) or Greenwich Mean Time (GMT).*

Select from the following:

- To view a summary of the daily web bandwidth usage, see "Viewing the Web Usage Summary Report" on page 27.
- To view a list of the top visited sites, see "Viewing the Top Sites" on page 29.
- To view the users who consume the most web bandwidth, see "Viewing the Top Users of HTTP Bandwidth" on page 30.
- To view the top sites visited by each user, see "Viewing HTTP Bandwidth Usage by User" on page 32.
- To view web bandwidth usage over a period of time, see "Viewing Bandwidth Usage Over Time" on page 33.
- To view a list of the top visited sites over time, see "Viewing Top Sites Over Time" on page 34.
- To view the users who consume the most web bandwidth over time, see "Viewing Top Users Over Time" on page 35.
- To view the top sites visited by each user over time, see "Viewing Bandwidth Usage By User Over Time" on page 37.

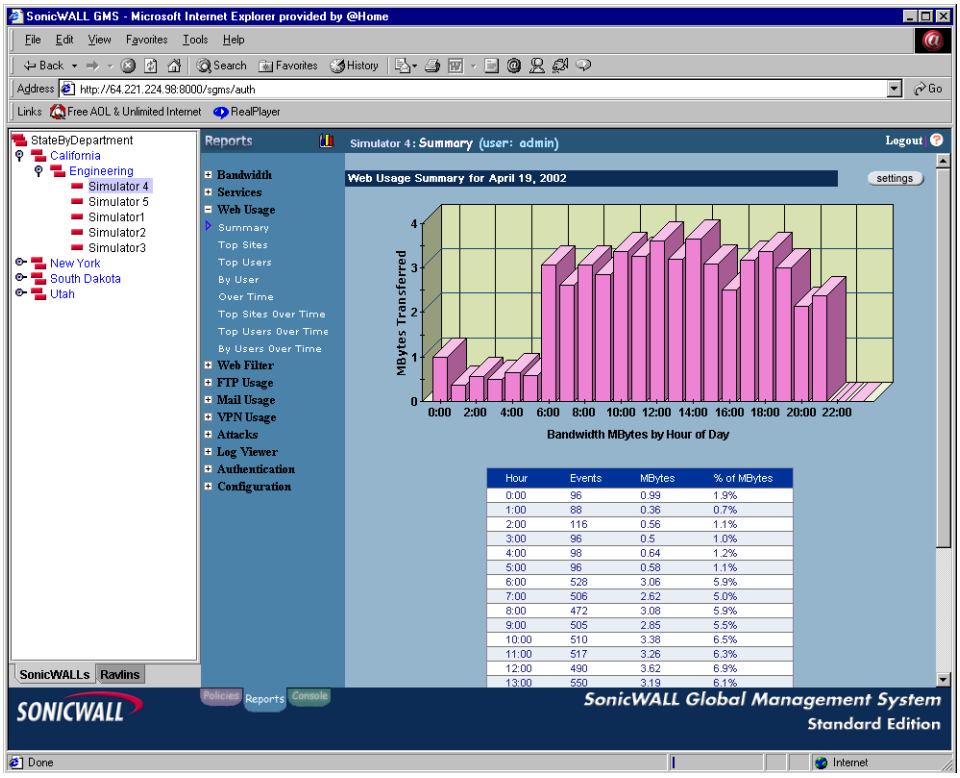
Viewing the Web Usage Summary Report

The Web Usage Summary report contains information on the amount of HTTP bandwidth handled by a SonicWALL appliance or group of SonicWALL appliances during each hour of the specified day.

To view the Web Usage Summary report, follow these steps:

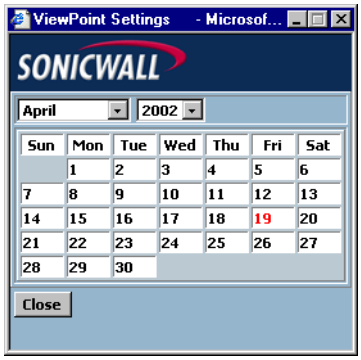
1. Start and log into ViewPoint.
2. Click the **Reports** tab.
3. Select the global icon, a group, or a SonicWALL appliance.
4. Expand the Web Usage tree and click **Summary**. The Summary page appears (Figure 19).

Figure 19: Summary Page



5. The bar graph displays the amount of HTTP bandwidth transferred during each hour of the day.
6. The table contains the following information:
   - **Hour**—when the sample was taken.
   - **Events**—number of events or "hits."
   - **MBytes**—number of megabytes transferred.
   - **% of MBytes**—percentage of megabytes transferred during this hour, compared to the day. For example, if 1000 megabytes of HTTP data was transferred during the day and 100 megabytes was transferred at the 12:00 time period, the **% of MBytes** field will display 10%.
7. The GMS Reporting Module shows today's report. To change the date of the report, click **Settings**. The Report Settings dialog box appears (Figure 20).

Figure 20: Report Settings Dialog Box


ViewPoint Settings - Microsof...
SONICWALL
April
2002
Sun Mon Tue Wed Thu Fri Sat
1 2 3 4 5 6
7 8 9 10 11 12 13
14 15 16 17 18 19 20
21 22 23 24 25 26 27
28 29 30
Close

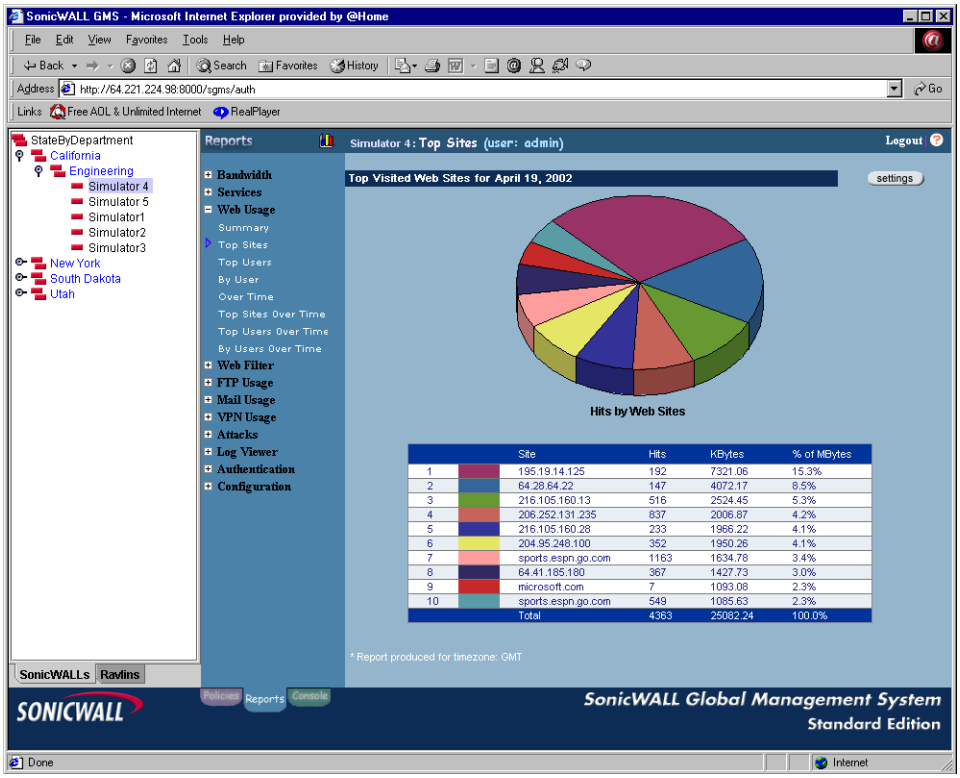
8. Select the year, month, and day that you would like to view.
9. When you are finished, click **Close.** The GMS Reporting Module displays the report for the selected day.

Viewing the Top Sites

The Top Sites report displays the web sites that used the most HTTP bandwidth on the specified date. To view the Top Sites report, follow these steps:

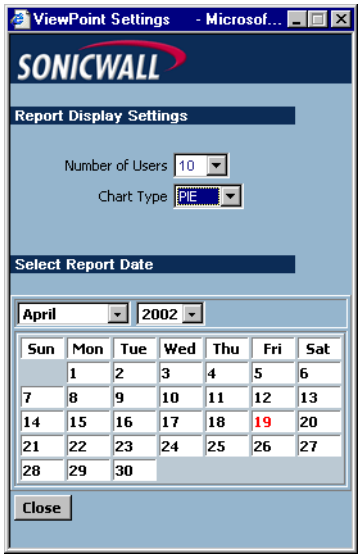
1. Start and log into ViewPoint.
2. Click the **Reports** tab.
3. Select a SonicWALL appliance.
4. Expand the Web Usage tree and click **Top Sites**. The Top Sites page appears (Figure 21).

Figure 21: Top Sites Page



5. The pie chart displays the percentage of bandwidth used to access the top sites.
6. The table contains the following information:
   - **Site**—URL or IP address of the site.
   - **Hits**—number of hits.
   - **MBytes**—number of megabytes transferred.
   - **% of MBytes**—percentage of megabytes transferred between this site, compared to all other HTTP traffic. For example, if 10,000 megabytes of data was transferred during the day and 5,000 megabytes was transferred between the appliance and Ebay, the **% of MBytes** field will display 50% and you have a problem.
7. By default, GMS Reporting shows today's report, a pie chart, and the ten top sites. To change these settings, click **Settings**. The Report Settings dialog box appears (Figure 22).

Figure 22: Report Settings Dialog Box


ViewPoint Settings - Microsof...
SONICWALL
Report Display Settings
Number of Users 10
Chart Type PIE
Select Report Date
April 2002
Sun Mon Tue Wed Thu Fri Sat
1 2 3 4 5 6
7 8 9 10 11 12 13
14 15 16 17 18 19 20
21 22 23 24 25 26 27
28 29 30
Close

8. Select the number of sites that will be displayed from the **Number of Sites** list box.
9. Select the type of chart from the **Chart Type** list box.
10. Select the year, month, and day that you would like to view.
11. When you are finished, click **Close.** The GMS Reporting Module displays the report for the selected day.

    Note: *These settings will stay in effect for all reports during your active login session.*

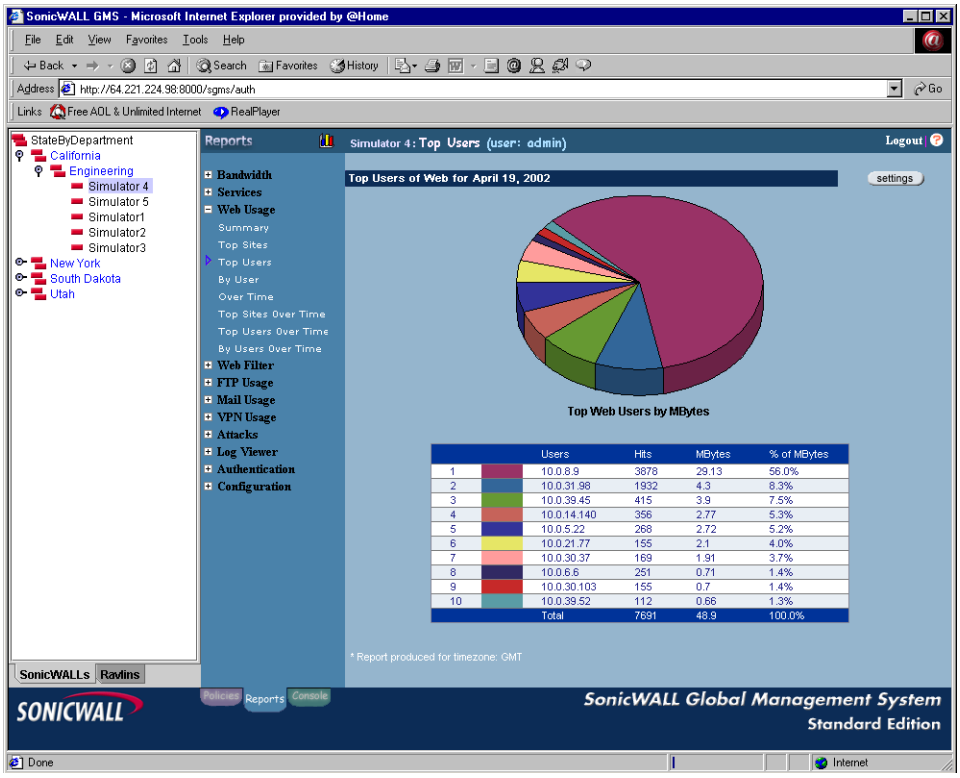
Viewing the Top Users of HTTP Bandwidth

The Top Users report displays the users who used the most HTTP bandwidth on the specified date.

To view the Top Users report, follow these steps:

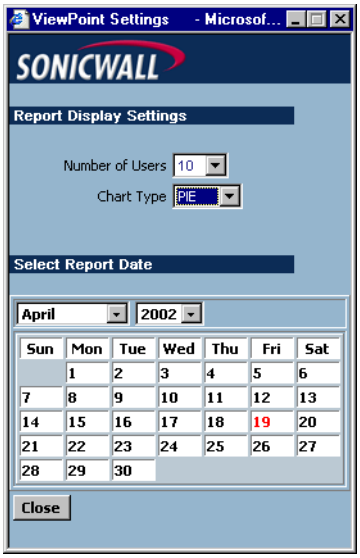
1. Start and log into ViewPoint.
2. Click the **Reports** tab.
3. Select a SonicWALL appliance.
4. Expand the Web Usage tree and click **Top Users**. The Top Users page appears (Figure 23).

Figure 23: Top Users Page



5. The pie chart displays the percentage of bandwidth transferred by each of the top users.
6. The table contains the following information:
   - **Users**—the IP address of the user.
   - **Hits**—number of hits.
   - **MBytes**—number of megabytes transferred.
   - **% of MBytes**—percentage of megabytes transferred by this user, compared to all users. For example, if 1000 megabytes of data was transferred during the day and 200 megabytes was transferred by the top user, the **% of MBytes** field will display 20%.
7. By default, GMS Reporting shows today's report, a pie chart, and the ten top users. To change these settings, click **Settings**. The Report Settings dialog box appears (Figure 24).

Figure 24: Report Settings Dialog Box


ViewPoint Settings - Microsof...
SONICWALL
Report Display Settings
Number of Users 10
Chart Type PIE
Select Report Date
April 2002
Sun Mon Tue Wed Thu Fri Sat
1 2 3 4 5 6
7 8 9 10 11 12 13
14 15 16 17 18 19 20
21 22 23 24 25 26 27
28 29 30
Close

8. Select the number of users that will be displayed from the **Number of Users** list box.
9. Select the type of chart from the **Chart Type** list box.
10. Select the year, month, and day that you would like to view.
11. When you are finished, click **Close.** The GMS Reporting Module displays the report for the selected day.

    Note: *These settings will stay in effect for all reports during your active login session.*

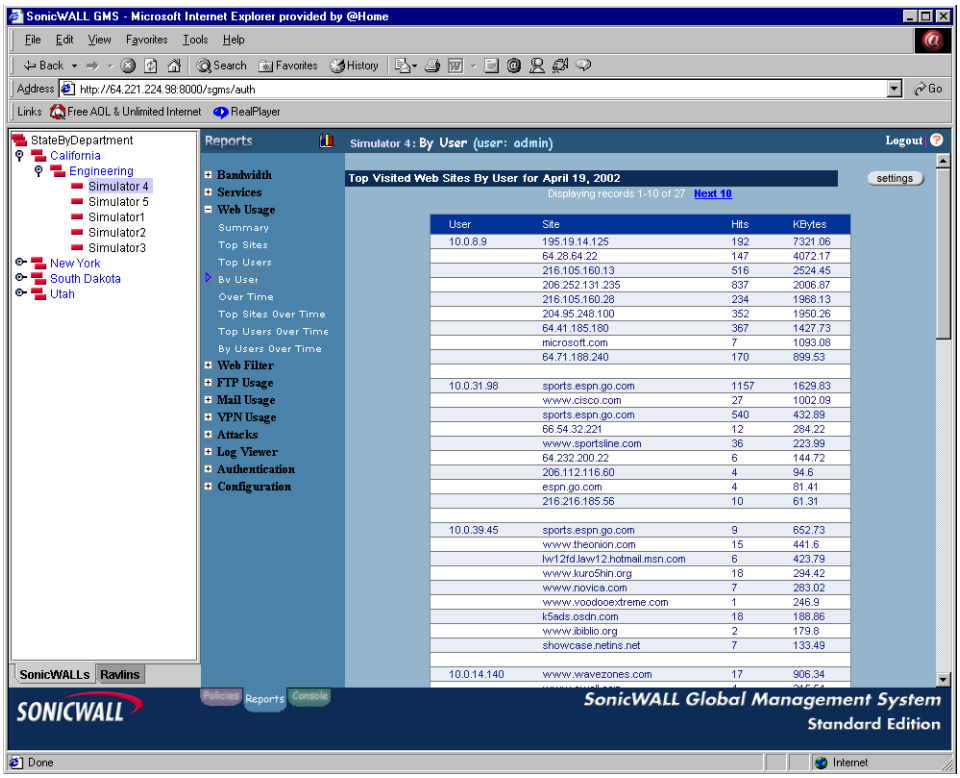
Viewing HTTP Bandwidth Usage by User

The By User report displays a list of all users, their top sites, the number of hits to each site, and the amount of data transferred.

To view the By User report, follow these steps:

1. Start and log into ViewPoint.
2. Click the **Reports** tab.
3. Select a SonicWALL appliance.
4. Expand the Web Usage tree and click **By User**. The By User page appears (Figure 25).

Figure 25: By User Page



5. The table contains the following information:
   - **User**—the IP address of the user.
   - **Site**—the top five sites visited by the user.
   - **Hits**—number of hits to each web site visited by the user.
   - **KBytes**—number of kilobytes transferred.
6. The GMS Reporting Module shows today's report. To change the date of the report, click **Settings**. The Report Settings dialog box appears.
7. Select the year, month, and day that you would like to view.
8. When you are finished, click **Close.** The GMS Reporting Module displays the report for the selected day.

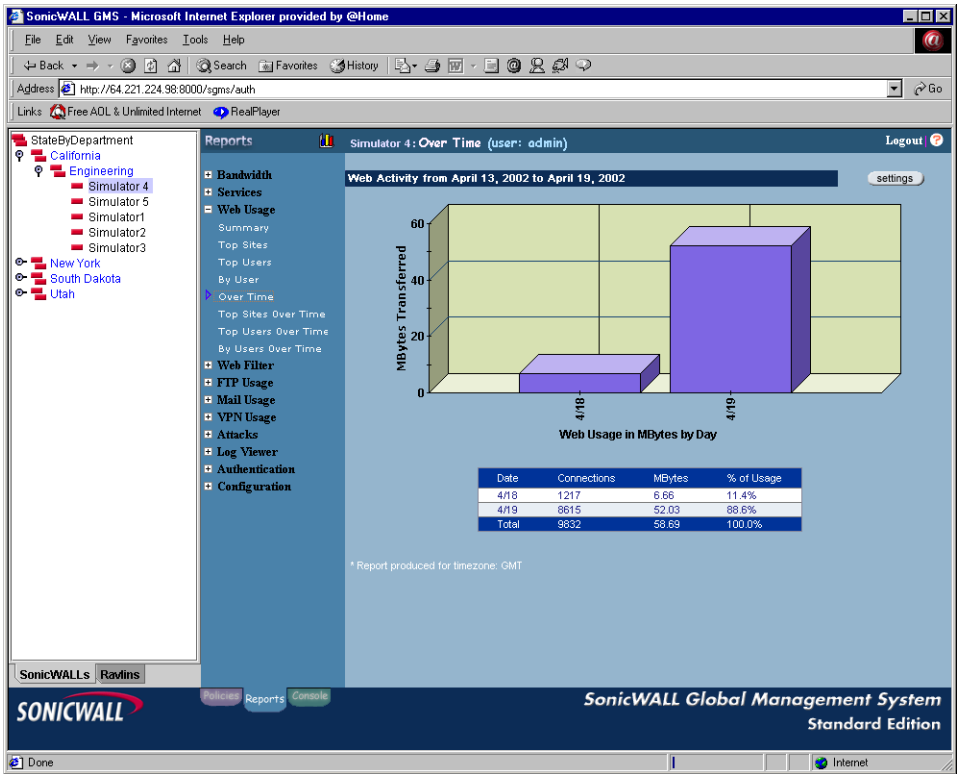
Viewing Bandwidth Usage Over Time

The Web Usage Over Time report displays the daily amount of HTTP bandwidth handled by a SonicWALL appliance or group of SonicWALL appliances for the specified time period.

To view the Web Usage Over Time report, follow these steps:

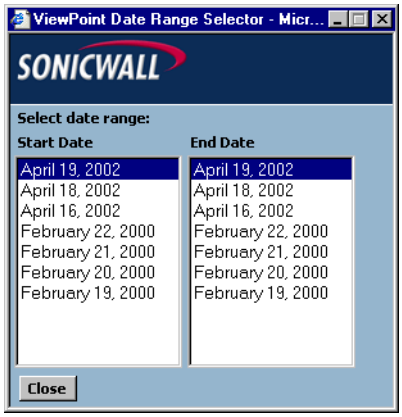
1. Start and log into ViewPoint.
2. Click the **Reports** tab.
3. Select the global icon, a group, or a SonicWALL appliance.
4. Expand the Web Usage tree and click **Over Time**. The Over Time page appears (Figure 26).

Figure 26: Over Time Page



5. The bar graph displays the amount of HTTP bandwidth transferred during each day of the specified time period.
6. The table contains the following information:
   - **Date**—when the sample was taken.
   - **Connections**—number of connections or hits.
   - **MBytes**—number of megabytes transferred.
   - **% of Usage**—percentage of megabytes transferred during this day, compared to the time period. For example, if 100,000 megabytes of data was transferred during the time period and 25,000 megabytes was transferred on one day, the **% of Usage** field will display 25%.
7. To change the date range of the report, click **Settings**. The Reporting Date Range Selector dialog box appears (Figure 27).

Figure 27: Report Settings Dialog Box



8. Select the starting and ending dates that you would like to view.
9. When you are finished, click **Close.** The GMS Reporting Module displays the report for the selected date range.

   Note: *These settings will stay in effect for all reports during your active login session.*

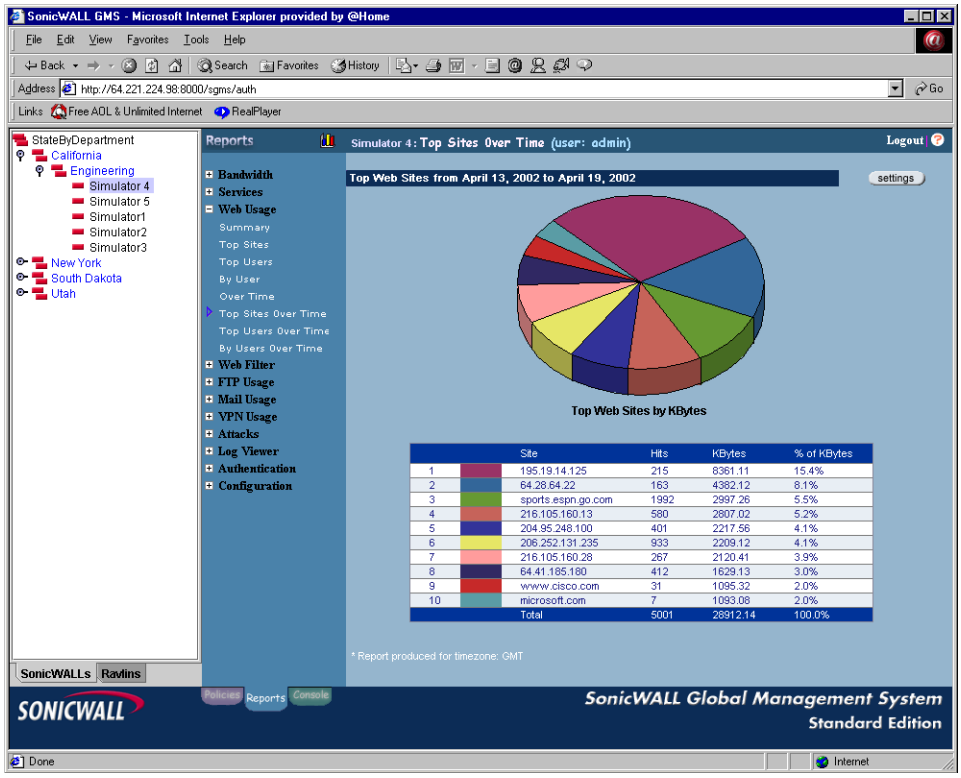
Viewing Top Sites Over Time

The Top Sites Over Time report displays the most visited web sites for the specified time period.

To view the Top Sites Over Time report, follow these steps:

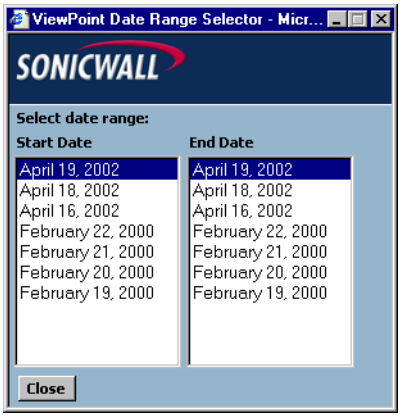
1. Start and log into ViewPoint.
2. Click the **Reports** tab.
3. Select a SonicWALL appliance.
4. Expand the Web Usage tree and click **Top Sites Over Time**. The Top Sites Over Time page appears (Figure 28).

Figure 28: Top Sites Over Time Page



5. The bar graph displays the amount of HTTP bandwidth transferred during each day of the specified time period.
6. The table contains the following information:
   - **Site**—URL or IP address of the site.
   - **Hits**—number of hits.
   - **KBytes**—number of kilobytes transferred.
   - **% of KBytes**—percentage of kilobytes transferred between this site, compared to all other HTTP traffic. For example, if 1,000,000 kilobytes of data was transferred during the day and 500,000 kilobytes was transferred between the appliance and Ebay, the **% of KBytes** field will display 50% and you have a problem.
7. To change the date range of the report, click **Settings**. The Reporting Date Range Selector dialog box appears (Figure 29).

Figure 29: Report Settings Dialog Box



8. Select the starting and ending dates that you would like to view.
9. When you are finished, click **Close.** The GMS Reporting Module displays the report for the selected date range.

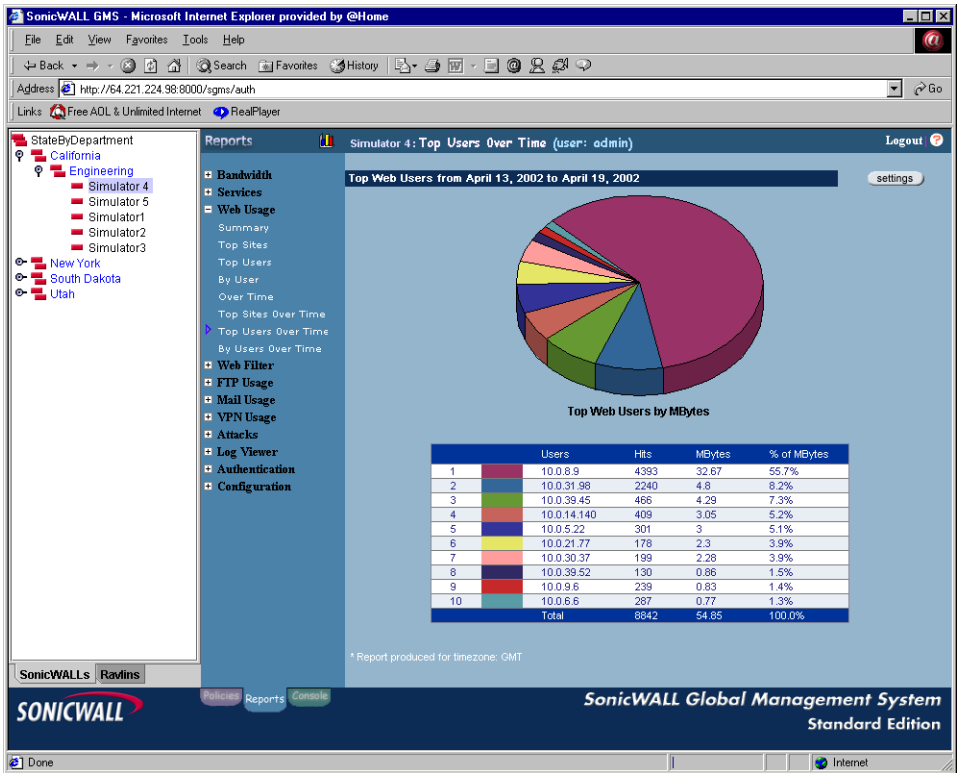
   Note: *These settings will stay in effect for all reports during your active login session.*

Viewing Top Users Over Time

The Top Users Over Time report displays the top users of bandwidth for the specified time period. To view the Top Users Over Time report, follow these steps:

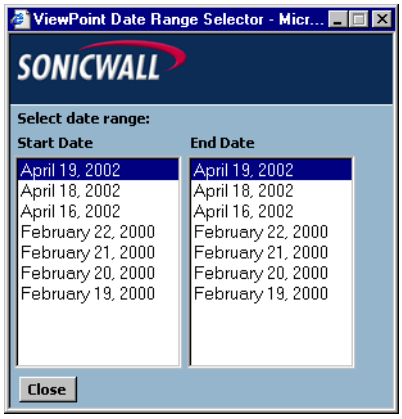
1. Start and log into ViewPoint.
2. Click the **Reports** tab.
3. Select a SonicWALL appliance.
4. Expand the Web Usage tree and click **Top Users Over Time**. The Top Users Over Time page appears (Figure 30).

Figure 30: Top Users Over Time Page



5. The graph provides a graphical display of the percentage of bandwidth transferred by each of the top users over the specified time period.
6. The table contains the following information:
   - **Users**—the IP address of the user.
   - **Hits**—number of hits.
   - **MBytes**—number of megabytes transferred.
   - **% of MBytes**—percentage of megabytes transferred by this user, compared to all users. For example, if 1000 megabytes of data was transferred during the period and 200 megabytes was transferred by the top user, the **% of MBytes** field will display 20%.
7. To change the date range of the report, click **Settings**. The Reporting Date Range Selector dialog box appears (Figure 31).

Figure 31: Report Settings Dialog Box



8. Select the starting and ending dates that you would like to view.
9. When you are finished, click **Close.** The GMS Reporting Module displays the report for the selected date range.

   Note: *These settings will stay in effect for all reports during your active login session.*

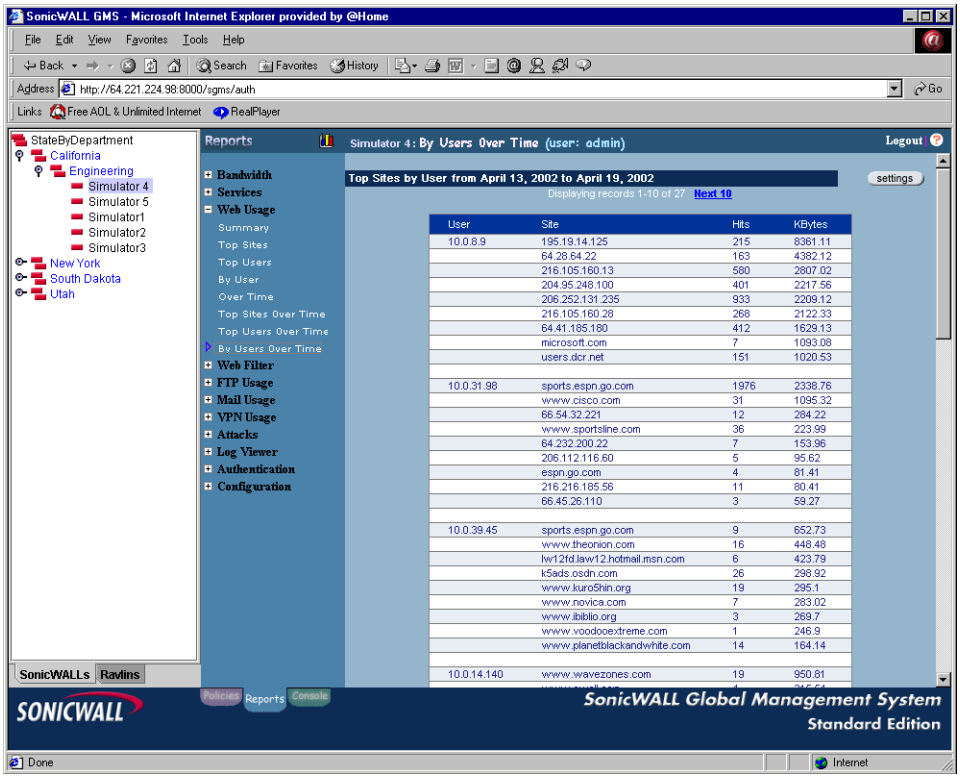
Viewing Bandwidth Usage By User Over Time

The By User Over Time report displays a list of all users, their top sites, the number of hits to each site, and the amount of data transferred for the specified time period.

To view the By User Over Time report, follow these steps:

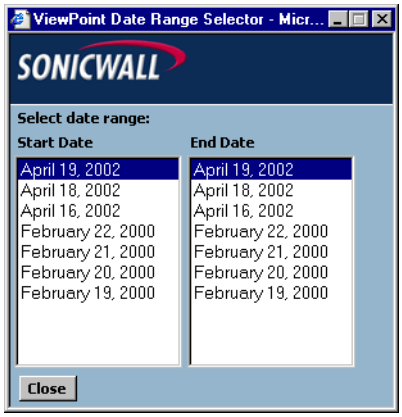
1. Start and log into ViewPoint.
2. Click the **Reports** tab.
3. Select a SonicWALL appliance.
4. Expand the Web Usage tree and click **By User Over Time**. The By User Over Time page appears (Figure 32).

Figure 32: By User Over Time Page



5. The bar graph displays the amount of HTTP bandwidth transferred during each day of the specified time period.
6. The table contains the following information:
   - User—the IP address of the user.
   - Site—the top five sites visited by the user.
   - Hits—number of hits to each web site visited by the user.
   - KBytes—number of kilobytes transferred.
7. To change the date range of the report, click **Settings**. The Reporting Date Range Selector dialog box appears (Figure 33).

Figure 33: Report Settings Dialog Box



8. Select the starting and ending dates that you would like to view.
9. When you are finished, click **Close.** The GMS Reporting Module displays the report for the selected date range.

   Note: *These settings will stay in effect for all reports during your active login session.*

Viewing Web Filter Reports

Web filter reports provide information on the number of attempts that users made to access blocked web sites through the selected SonicWALL appliance(s). These reports include web sites blocked by the Content Filter List, customized keyword filtering, and domain name filtering.

Web filter reports can be used to view blocked site access attempts by the hour, day, or over a period of days. Additionally, you can view the users that most frequently attempt to access blocked sites and the most popular blocked sites.

Note: *All reports appear in Universal Time, Coordinated (UTC) or Greenwich Mean Time (GMT).*

Select from the following:

- To view a summary of the blocked site access attempts, see "Viewing the Web Filter Summary Report" on page 39.
- To view a list of the blocked sites that users attempted to access most often, see "Viewing the Web Filter Top Sites Report" on page 40.
- To view the users who made the most attempts to access blocked sites, see "Viewing the Top Users that Try to Access Blocked Sites" on page 42.
- To view the top blocked sites that each user attempted to access, see "Viewing the Top Blocked Sites for Each User" on page 43.
- To view blocked site access attempts over a period of time, see "Viewing Blocked Site Attempts Over Time" on page 45.
- To view a list of the blocked sites that users attempted to access most often over time, see "Viewing Blocked Site Attempts Over Time" on page 45.
- To view the users who made the most attempts to access blocked sites over time, see "Viewing the Top Blocked Site Users Over Time" on page 47.
- To view the top blocked sites that each user attempted to access over time, see "Viewing the Top Blocked Sites for Each User Over Time" on page 49.

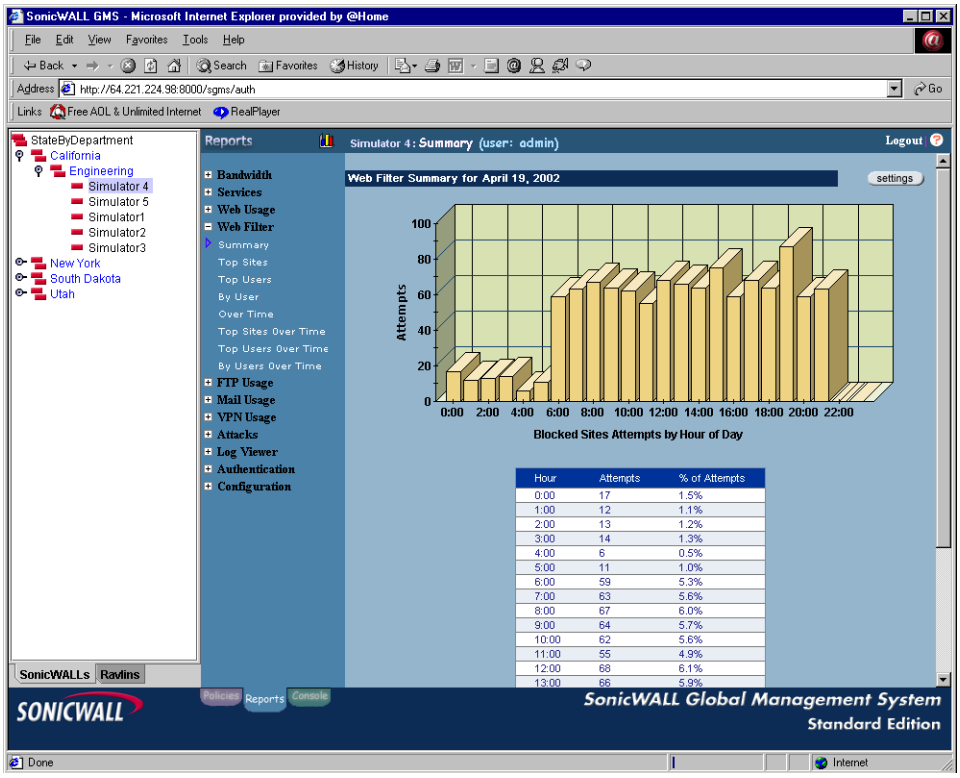
Viewing the Web Filter Summary Report

The Web Filter Summary report contains information on the number of times users attempt to access blocked sites for the specified day.

To view the Web Filter Summary report, follow these steps:

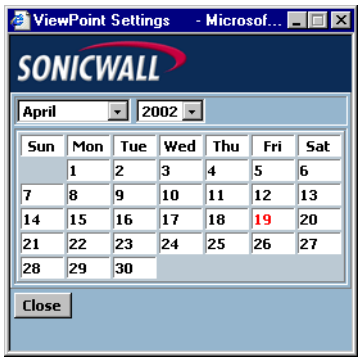
1. Start and log into ViewPoint.
2. Click the **Reports** tab.
3. Select the global icon, a group, or a SonicWALL appliance.
4. Expand the Web Filter tree and click **Summary**. The Summary page appears (Figure 34).

Figure 34: Summary Page



5. The bar graph displays the number of blocked sites that users attempted to access during each hour of the day.
6. The table contains the following information:
   - **Hour**—time when the sample was taken.
   - **Attempts**—number of attempts to access blocked sites.
   - **% of Attempts**—percentage of attempts during this hour, compared to the day. For example, if 100 attempts occurred during the day and 20 attempts occurred at the 12:00 time period, the **% of Attempts** field will display 20%.
7. The GMS Reporting Module shows today's report. To change the date of the report, click **Settings**. The Report Settings dialog box appears (Figure 35).

Figure 35: Report Settings Dialog Box


ViewPoint Settings - Microsof...
SONICWALL
April
2002
Sun Mon Tue Wed Thu Fri Sat
1 2 3 4 5 6
7 8 9 10 11 12 13
14 15 16 17 18 19 20
21 22 23 24 25 26 27
28 29 30
Close

8. Select the year, month, and day that you would like to view.
9. When you are finished, click **Close.** The GMS Reporting Module displays the report for the selected day.

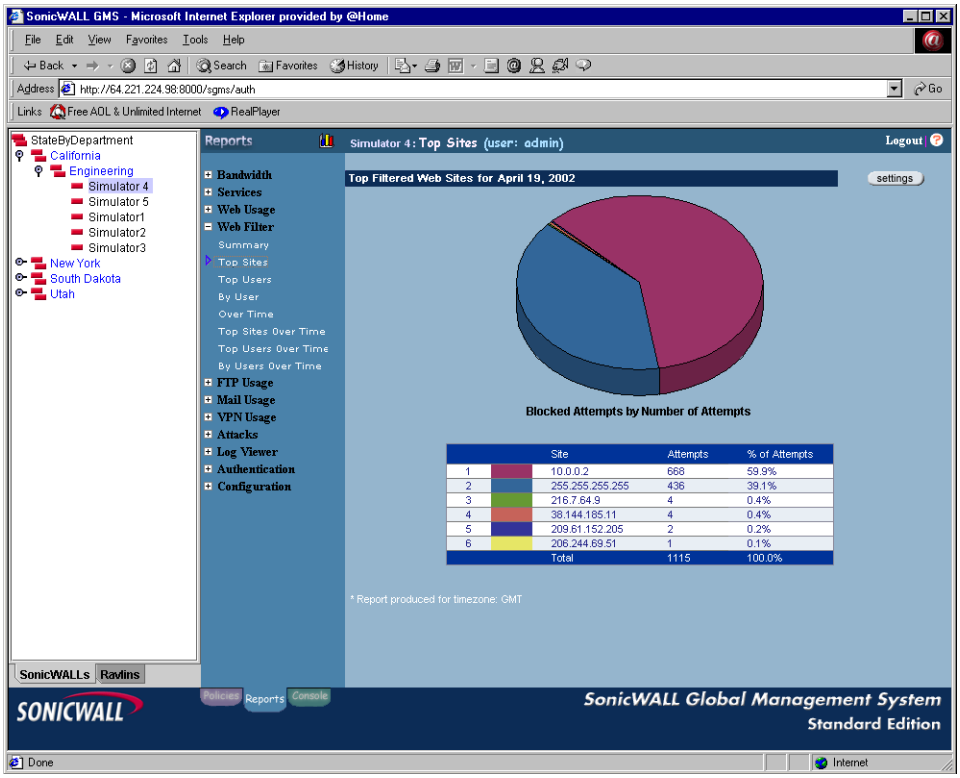
Viewing the Web Filter Top Sites Report

The Web Filter Top Sites report displays the top blocked web sites that users attempted to access on the specified date.

To view the Top Sites report, follow these steps:

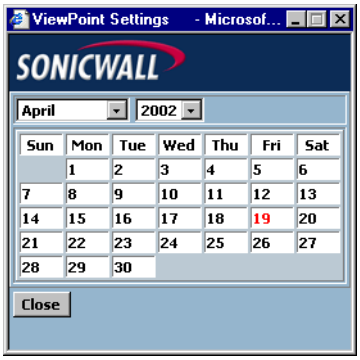
1. Start and log into ViewPoint.
2. Click the **Reports** tab.
3. Select a SonicWALL appliance.
4. Expand the Web Filter tree and click **Top Sites**. The Top Sites page appears (Figure 36).

Figure 36: Top Sites Page



5. The graph provides a display of the number of access attempts for each of the top twenty blocked web sites.
6. The table contains the following information:
   - **Site**—URL or IP address of the site.
   - **Attempts**—number of attempts.
   - **% of Attempts**—percentage of attempts to access the blocked site, compared to all other blocked site attempts. For example, if 500 attempts were made during the day and 100 of those attempts were for www.badsite.com, its **% of Attempts** field will display 20%.
7. The GMS Reporting Module shows today's report. To change the date of the report, click **Settings**. The Report Settings dialog box appears (Figure 37).

Figure 37: Report Settings Dialog Box


ViewPoint Settings - Microsof...
SONICWALL
April
2002
Sun Mon Tue Wed Thu Fri Sat
1 2 3 4 5 6
7 8 9 10 11 12 13
14 15 16 17 18 19 20
21 22 23 24 25 26 27
28 29 30
Close

8. Select the year, month, and day that you would like to view.
9. When you are finished, click **Close.** The GMS Reporting Module displays the report for the selected day.

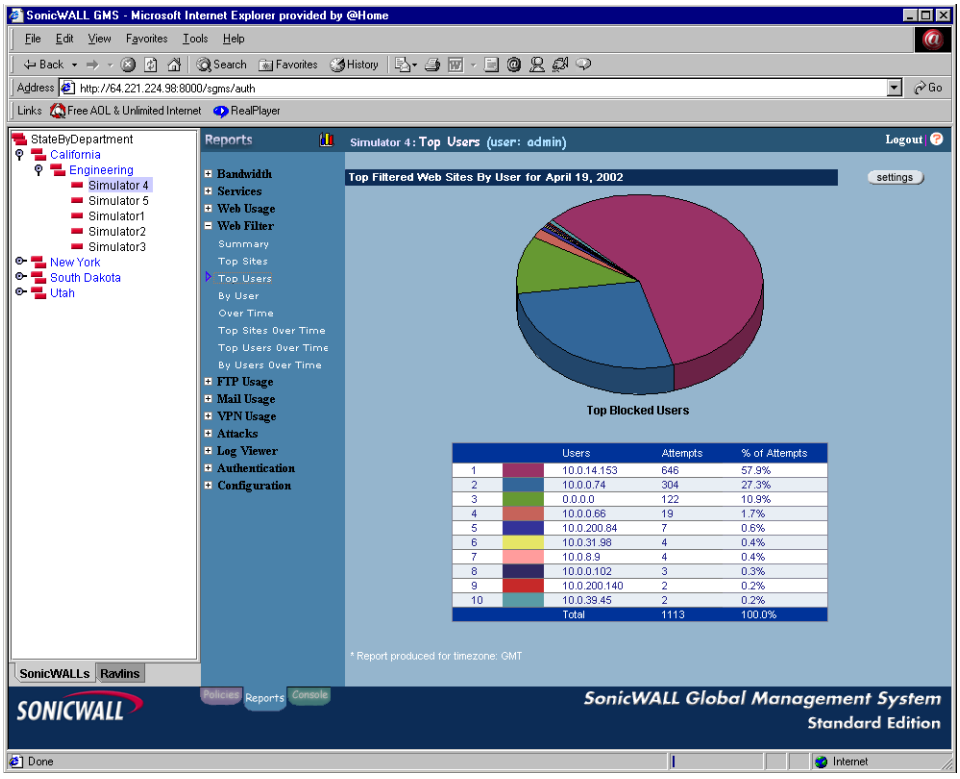
Viewing the Top Users that Try to Access Blocked Sites

The Web Filter Top Users report displays the users who made the most attempts to access blocked sites on the specified date.

To view the Top Users report, follow these steps:

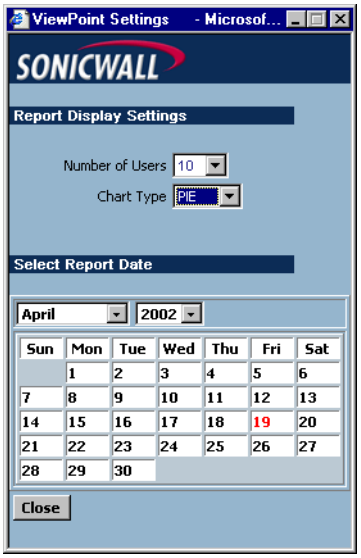
1. Start and log into ViewPoint.
2. Click the **Reports** tab.
3. Select a SonicWALL appliance.
4. Expand the Web Filter tree and click **Top Users**. The Top Users page appears (Figure 38).

Figure 38: Top Users Page



5. The pie chart displays the top users with the most blocked site attempts.
6. The table contains the following information:
   - **Users**—the IP address of the user.
   - **Attempts**—number of attempts.
   - **% of Attempts**—percentage of attempts to access the blocked site, compared to all other user attempts. For example, if 500 attempts were made during the day and 250 of those attempts were made by a single user, his **% of Attempts** field will display 50%.
7. By default, GMS Reporting shows today's report, a pie chart, and the ten top users. To change these settings, click **Settings**. The Report Settings dialog box appears (Figure 39).

Figure 39: Report Settings Dialog Box


ViewPoint Settings - Microsof...
SONICWALL
Report Display Settings
Number of Users 10
Chart Type PIE
Select Report Date
April 2002
Sun Mon Tue Wed Thu Fri Sat
1 2 3 4 5 6
7 8 9 10 11 12 13
14 15 16 17 18 19 20
21 22 23 24 25 26 27
28 29 30
Close

8. Select the number of users that will be displayed from the **Number of Users** list box.
9. Select the type of chart from the **Chart Type** list box.
10. Select the year, month, and day that you would like to view.
11. When you are finished, click **Close.** The GMS Reporting Module displays the report for the selected day.

    Note: *These settings will stay in effect for all reports during your active login session.*

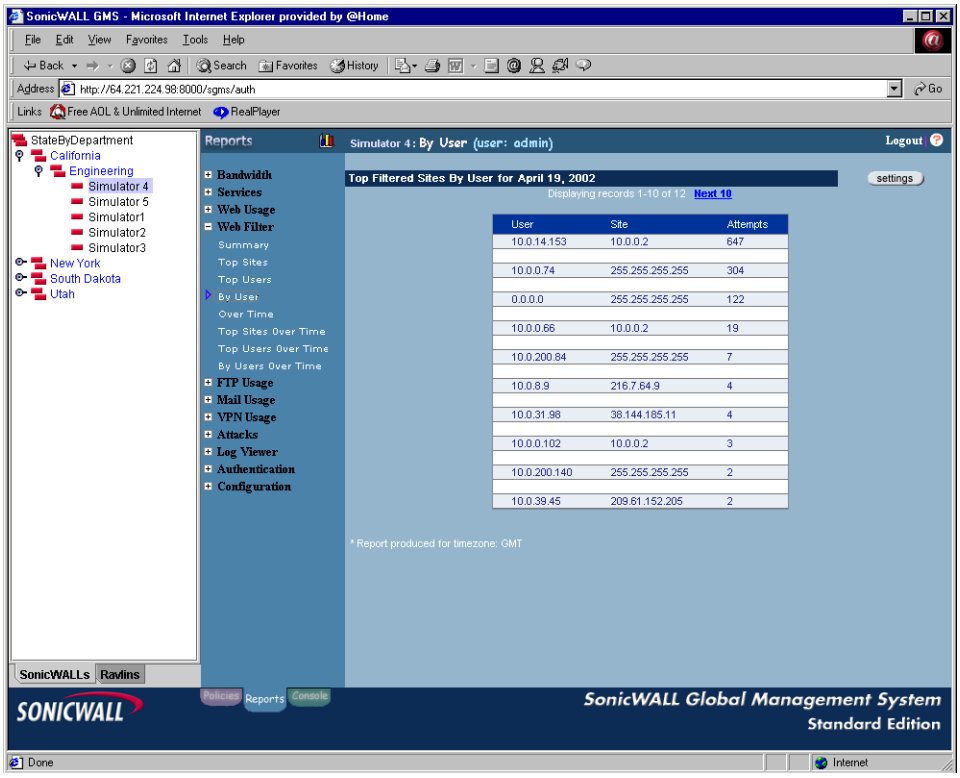
Viewing the Top Blocked Sites for Each User

The Web Filter By User report displays the top blocked web sites that each user attempted to access on the specified date.

To view the Web Filter By User report, follow these steps:

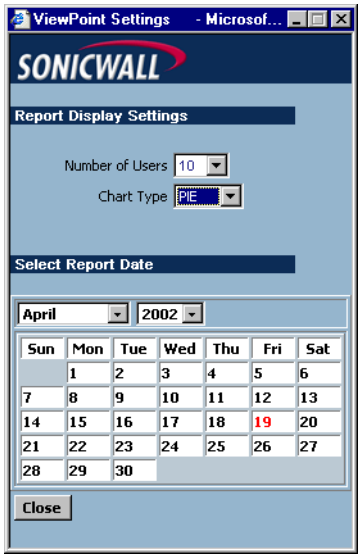
1. Start and log into ViewPoint.
2. Click the **Reports** tab.
3. Select a SonicWALL appliance.
4. Expand the Web Filter tree and click **By User**. The By User page appears (Figure 40).

Figure 40: By User Page



5. The table contains the following information:
   - User—the IP address of the user.
   - Site—the top five sites visited by the user.
   - Attempts—number of attempts the user made to access each web site.
6. By default, the GMS Reporting Module shows today's report, a pie chart, and the ten top users. To change these settings, click **Settings**. The Report Settings dialog box appears (Figure 41).

Figure 41: Report Settings Dialog Box


ViewPoint Settings - Microsof...
SONICWALL
Report Display Settings
Number of Users 10
Chart Type PIE
Select Report Date
April 2002
Sun Mon Tue Wed Thu Fri Sat
1 2 3 4 5 6
7 8 9 10 11 12 13
14 15 16 17 18 19 20
21 22 23 24 25 26 27
28 29 30
Close

7. Select the number of users that will be displayed from the **Number of Users** list box.
8. Select the type of chart from the **Chart Type** list box.
9. Select the year, month, and day that you would like to view.

10. When you are finished, click **Close.** The GMS Reporting Module displays the report for the selected day.

    Note: *These settings will stay in effect for all reports during your active login session.*

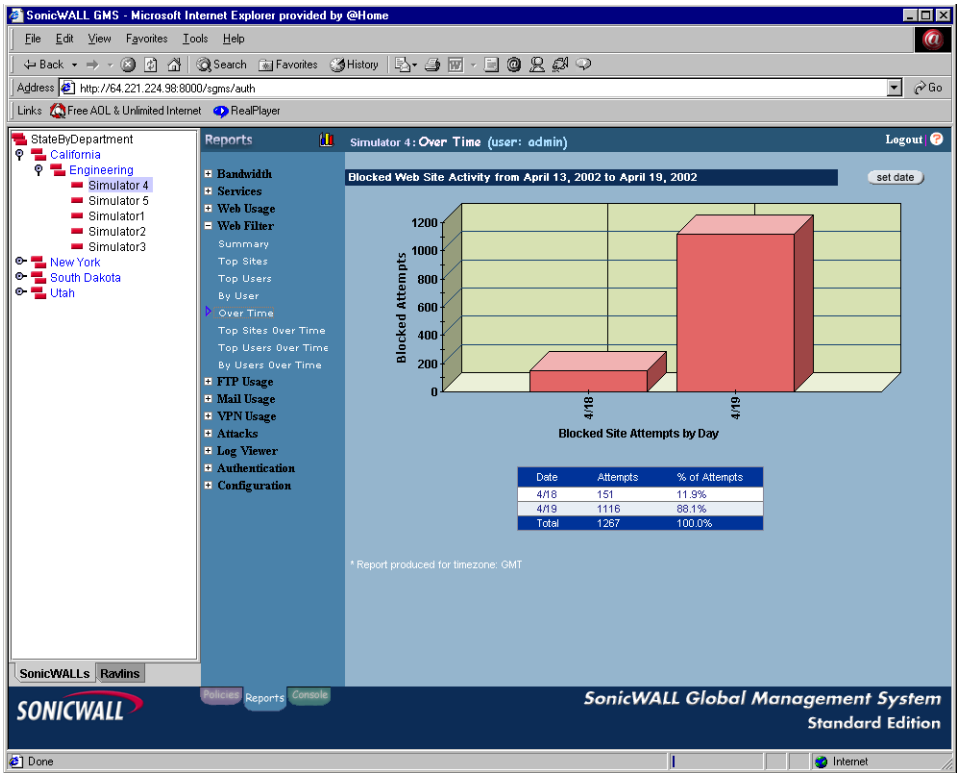
Viewing Blocked Site Attempts Over Time

The Web Filter Over Time report displays the number of attempts that were made to access blocked web sites for the specified time period.

To view the Web Filter Over Time report, follow these steps:

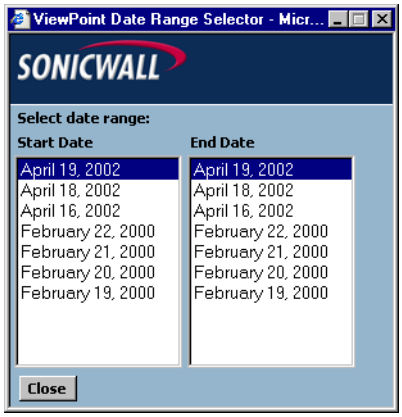
1. Start and log into ViewPoint.
2. Click the **Reports** tab.
3. Select the global icon, a group, or a SonicWALL appliance.
4. Expand the Web Filter tree and click **Over Time**. The Over Time page appears (Figure 42).

Figure 42: Over Time Page


SonicWALL GMS - Microsoft Internet Explorer provided by @Home
Simulator 4: Over Time (user: admin)
Logout
Blocked Web Site Activity from April 13, 2002 to April 19, 2002
set date
Blocked Attempts
Blocked Site Attempts by Day
Date Attempts % of Attempts
4/18 151 11.9%
4/19 1116 88.1%
Total 1267 100.0%
* Report produced for timezone: GMT
SonicWALL Global Management System
Standard Edition

5. The bar graph displays the number of attempts that were made to access blocked web sites during each day of the specified time period.
6. The table contains the following information:
   - **Date**—day when the sample was taken.
   - **Attempts**—number of attempts to access blocked web sites.
   - **% of Attempts**—percentage of attempts to access the blocked site on the day, compared to the time period. For example, if 5,000 attempts were made during the time period and 500 were made on one day, its **% of Attempts** field will display 10%.
7. To change the date range of the report, click **Settings**. The Reporting Date Range Selector dialog box appears (Figure 43).

Figure 43: Report Settings Dialog Box



8. Select the starting and ending dates that you would like to view.
9. When you are finished, click **Close.** The GMS Reporting Module displays the report for the selected date range.

   Note: *These settings will stay in effect for all reports during your active login session.*

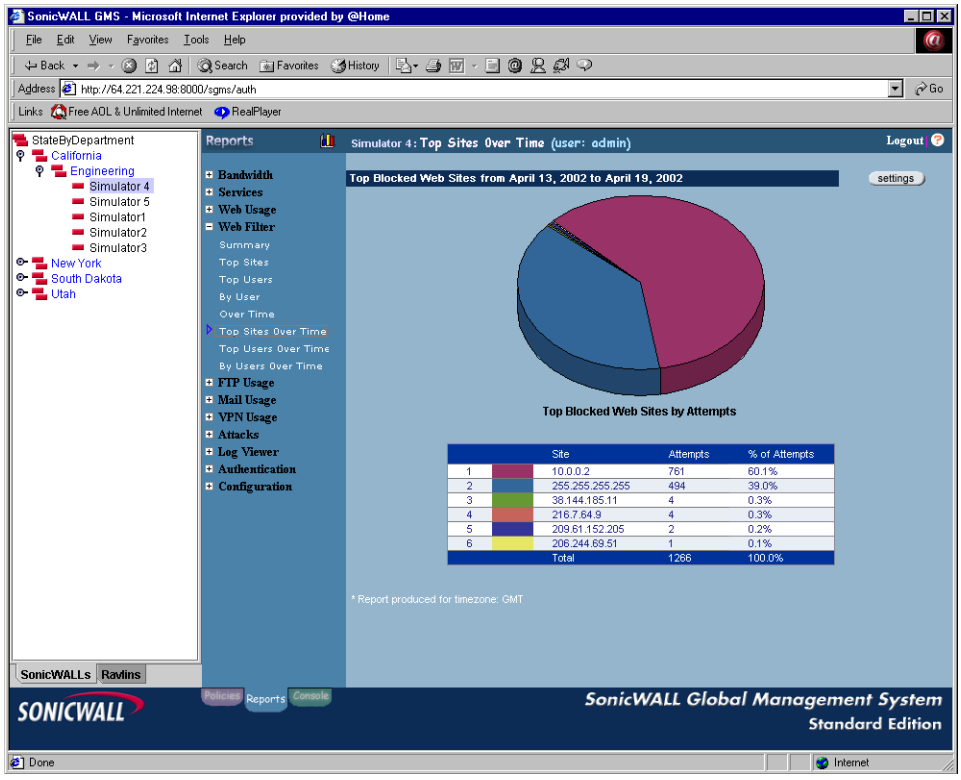
Viewing the Top Blocked Site Attempts Over Time

The Top Sites Over Time report displays the top blocked web sites for the specified time period.

To view the Web Filter Over Time report, follow these steps:

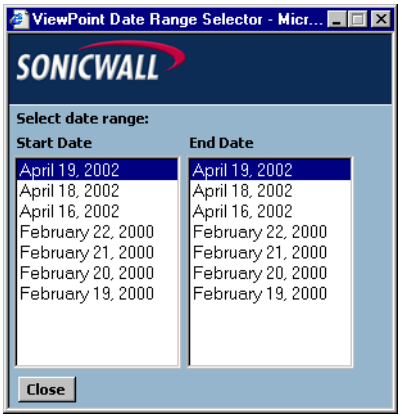
1. Start and log into ViewPoint.
2. Click the **Reports** tab.
3. Select a SonicWALL appliance.
4. Expand the Web Filter tree and click **Top Sites Over Time**. The Top Sites Over Time page appears (Figure 44).

Figure 44: Top Sites Over Time Page



5. The graph displays the number of access attempts for each of the top blocked web sites during the specified time period.
6. The table contains the following information:
   - **Site**—URL or IP address of the site.
   - **Attempts**—number of attempts.
   - **% of Attempts**—percentage of attempts to access the blocked site, compared to all other blocked site attempts. For example, if 500 attempts were made during the period and 100 of those attempts were for www.badsite.com, its **% of Attempts** field will display 20%.
7. To change the date range of the report, click **Settings**. The Reporting Date Range Selector dialog box appears (Figure 45).

   Figure 45: Report Settings Dialog Box



8. Select the starting and ending dates that you would like to view.
9. When you are finished, click **Close.** The GMS Reporting Module displays the report for the selected date range.

   Note: *These settings will stay in effect for all reports during your active login session.*

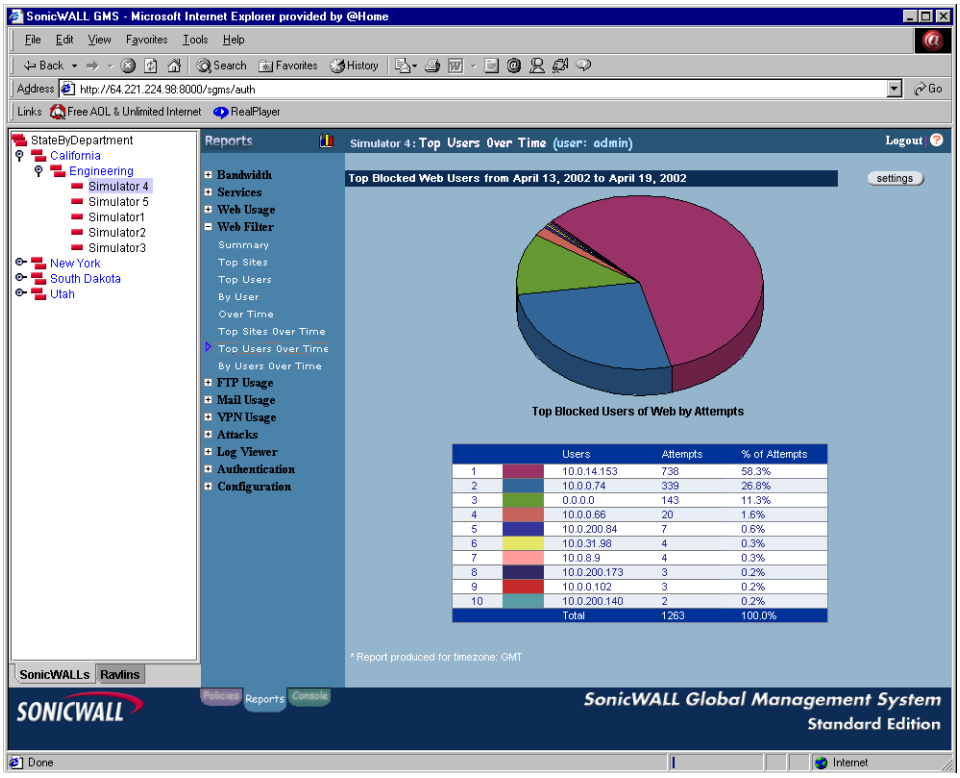
Viewing the Top Blocked Site Users Over Time

The Web Filter Top Users Over Time report displays the users who made the most attempts to access blocked sites during the specified time period.

To view the Top Users Over Time report, follow these steps:

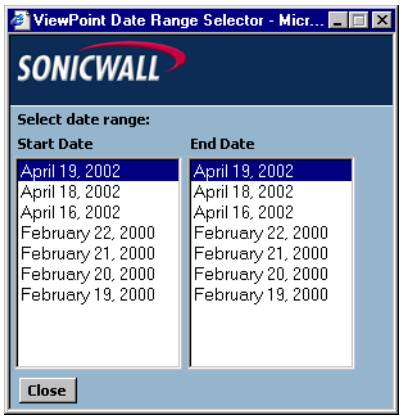
1. Start and log into ViewPoint.
2. Click the **Reports** tab.
3. Select a SonicWALL appliance.
4. Expand the Web Filter tree and click **Top Users Over Time**. The Top Users Over Time page appears (Figure 46).

Figure 46: Top Users Over Time Page



5. The pie chart displays the top users with the most blocked site attempts.
6. The table contains the following information:
   - **Users**—the IP address of the user.
   - **Attempts**—number of attempts.
   - **% of Attempts**—percentage of attempts to access the blocked site, compared to all other user attempts. For example, if 500 attempts were made during the period and 250 of those attempts were made by a single user, his **% of Attempts** field will display 50%.
7. To change the date range of the report, click **Settings**. The Reporting Date Range Selector dialog box appears (Figure 47).

Figure 47: Report Settings Dialog Box



8. Select the starting and ending dates that you would like to view.
9. When you are finished, click **Close.** The GMS Reporting Module displays the report for the selected date range.

   Note: *These settings will stay in effect for all reports during your active login session.*

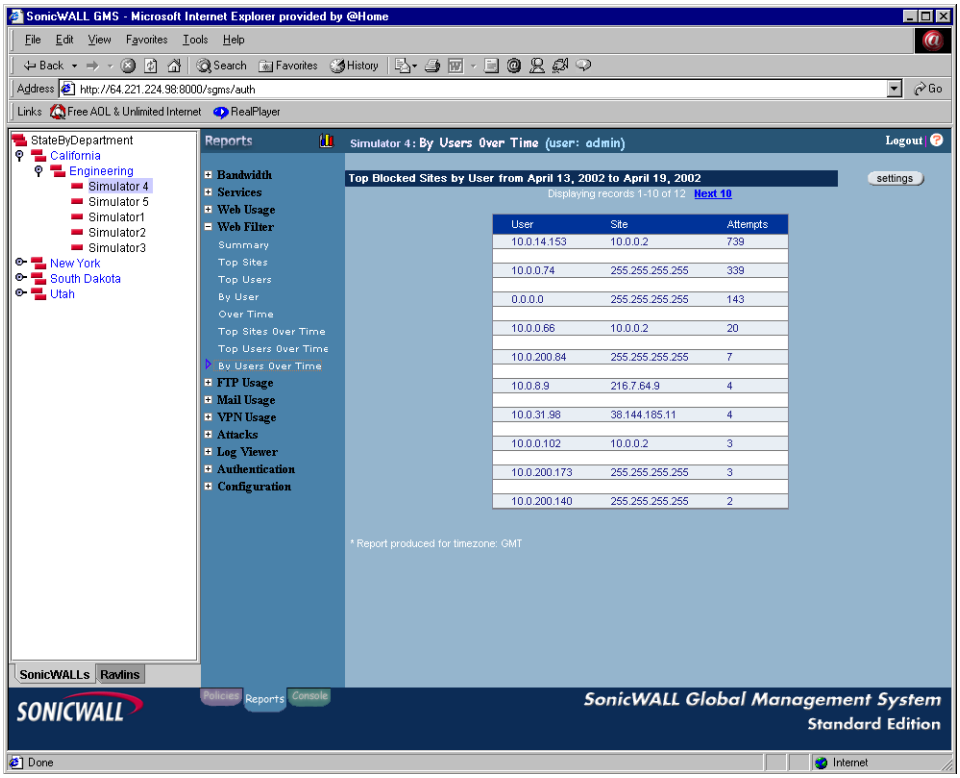
Viewing the Top Blocked Sites for Each User Over Time

The Web Filter By User report displays the top blocked web sites that each user attempted to access during the specified time period.

To view the By User Over Time report, follow these steps:

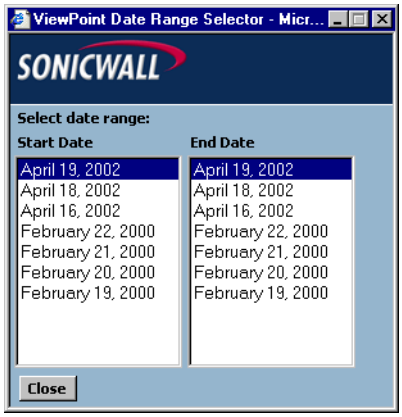
1. Start and log into ViewPoint.
2. Click the **Reports** tab.
3. Select a SonicWALL appliance.
4. Expand the Web Filter tree and click **By User Over Time**. The By User Over Time page appears (Figure 40).

Figure 48: By User Page



5. The table contains the following information:
   - User—the IP address of the user.
   - Site—the top five sites visited by the user.
   - Attempts—number of attempts the user made to access each web site.
6. To change the date range of the report, click **Settings**. The Reporting Date Range Selector dialog box appears (Figure 49).

Figure 49: Report Settings Dialog Box



7. Select the starting and ending dates that you would like to view.
8. When you are finished, click **Close.** The GMS Reporting Module displays the report for the selected date range.

   Note: *These settings will stay in effect for all reports during your active login session.*

Viewing File Transfer Protocol Reports

FTP usage reports provide information on the amount of FTP usage that occurs through the selected SonicWALL appliance(s).

FTP usage reports can be used to view FTP bandwidth usage by the hour, day, or over a period of days. Additionally, you can view the top users of FTP bandwidth.

General bandwidth reports do not always provide a complete picture of network bandwidth usage. If a large amount of FTP traffic occurs during peak times, you might need more bandwidth, you might need to upgrade network equipment, or you might ask employees to use compression or transfer large files during non-peak times.

Note: *All reports appear in Universal Time, Coordinated (UTC) or Greenwich Mean Time (GMT).*

Select from the following:

- To view a summary of the daily FTP bandwidth usage, see "Viewing the FTP Summary Report" on page 51.
- To view the users who consume the most FTP bandwidth, see "Viewing the Top Users of FTP Bandwidth" on page 52.
- To view FTP bandwidth usage over a period of time, see "Viewing FTP Bandwidth Usage Over Time" on page 54.
- To view the users who consume the most FTP bandwidth over time, see "Viewing FTP Bandwidth Usage Over Time" on page 54.

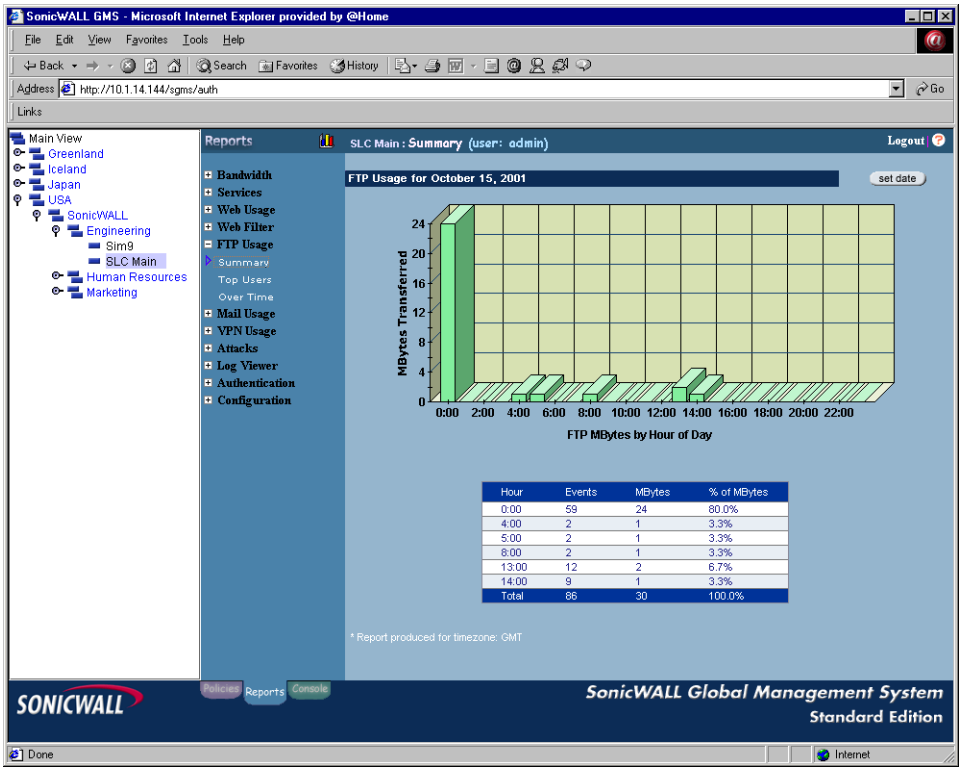
Viewing the FTP Summary Report

The FTP Summary report contains information on the amount of FTP bandwidth handled by a SonicWALL appliance or group of SonicWALL appliances during the specified day.

To view the FTP Summary report, follow these steps:

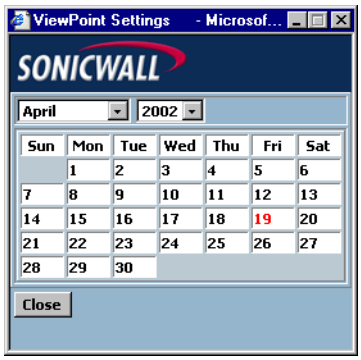
1. Start and log into ViewPoint.
2. Click the **Reports** tab.
3. Select the global icon, a group, or a SonicWALL appliance.
4. Expand the FTP Usage tree and click **Summary**. The Summary page appears (Figure 50).

Figure 50: Summary Page



5. The bar graph displays the amount of FTP bandwidth transferred during each hour of the day.
6. The table contains the following information:
   - **Hour**—when the sample was taken.
   - **Events**—number of FTP events.
   - **MBytes**—number of megabytes transferred.
   - **% of MBytes**—percentage of megabytes transferred during this hour, compared to the day. For example, if 1000 megabytes of FTP data was transferred during the day and 100 megabytes was transferred at the 12:00 time period, the **% of MBytes** field will display 10%.
7. The GMS Reporting Module shows today's report. To change the date of the report, click **Settings**. The Report Settings dialog box appears (Figure 51).

Figure 51: Report Settings Dialog Box


ViewPoint Settings - Microsof...
SONICWALL
April
2002
Sun Mon Tue Wed Thu Fri Sat
1 2 3 4 5 6
7 8 9 10 11 12 13
14 15 16 17 18 19 20
21 22 23 24 25 26 27
28 29 30
Close

8. Select the year, month, and day that you would like to view.
9. When you are finished, click **Close.** The GMS Reporting Module displays the report for the selected day.

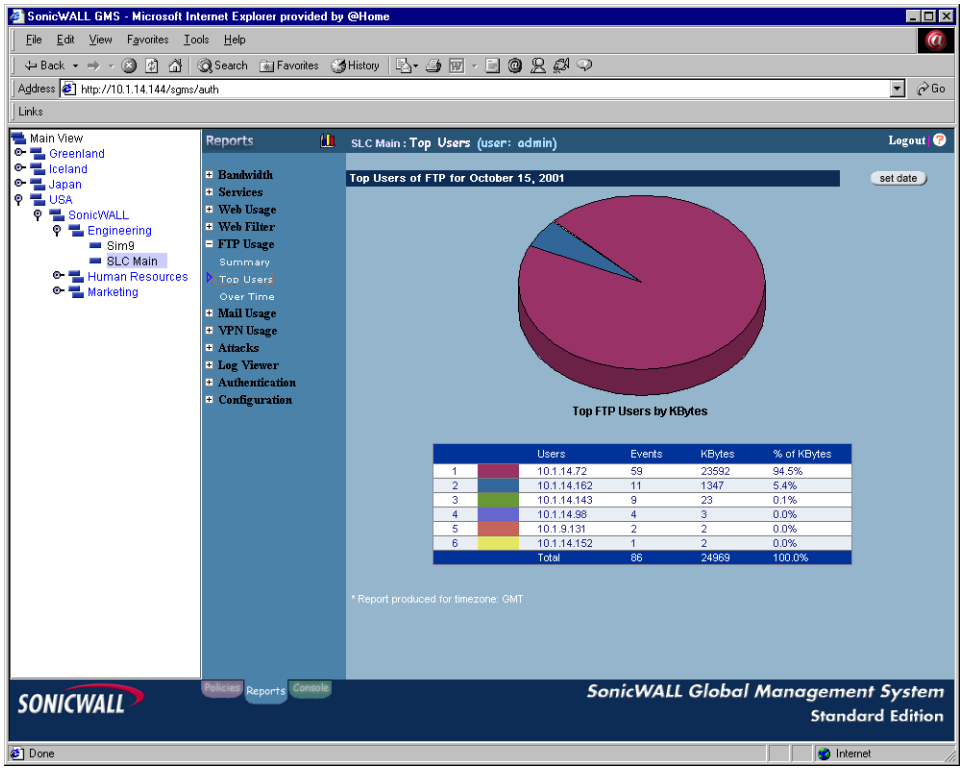
Viewing the Top Users of FTP Bandwidth

The Top Users report displays the users who used the most FTP bandwidth on the specified date.

To view the Top Users report, follow these steps:

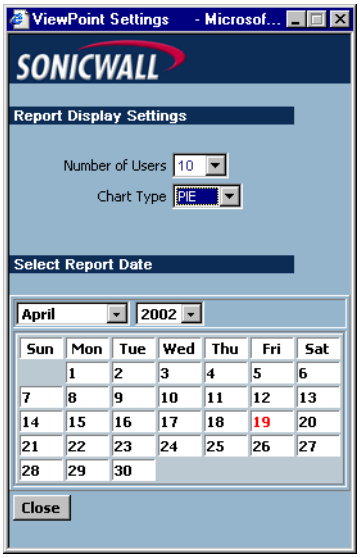
1. Start and log into ViewPoint.
2. Click the **Reports** tab.
3. Select a SonicWALL appliance.
4. Expand the FTP Usage tree and click **Top Users**. The Top Users page appears (Figure 52).

Figure 52: Top Users Page



5. The pie chart displays the percentage of bandwidth used by each user.
6. The table contains the following information:
   - **Users**—the IP address of the user.
   - **Events**—number of FTP Events.
   - **KBytes**—number of kilobytes transferred.
   - **% of KBytes**—percentage of kilobytes transferred by this user, compared to all users. For example, if 10000 kilobytes of data was transferred during the day and 2000 kilobytes was transferred by the top user, the **% of KBytes** field will display 20%.
7. By default, the GMS Reporting Module shows today's report, a pie chart, and the ten top users. To change these settings, click **Settings**. The Report Settings dialog box appears (Figure 53).

Figure 53: Report Settings Dialog Box


ViewPoint Settings - Microsof...
SONICWALL
Report Display Settings
Number of Users 10
Chart Type PIE
Select Report Date
April 2002
Sun Mon Tue Wed Thu Fri Sat
1 2 3 4 5 6
7 8 9 10 11 12 13
14 15 16 17 18 19 20
21 22 23 24 25 26 27
28 29 30
Close

8. Select the number of users that will be displayed from the **Number of Users** list box.
9. Select the type of chart from the **Chart Type** list box.
10. Select the year, month, and day that you would like to view.
11. When you are finished, click **Close.** The GMS Reporting Module displays the report for the selected day.

    Note: *These settings will stay in effect for all reports during your active login session.*

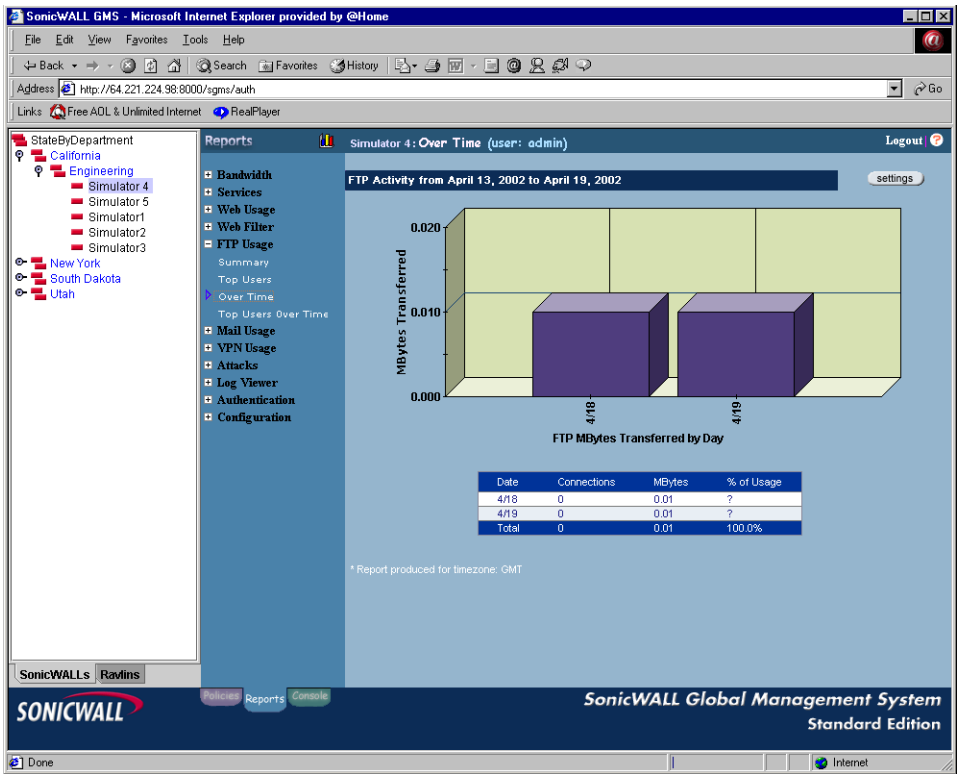
Viewing FTP Bandwidth Usage Over Time

The FTP Usage Over Time report displays the daily amount of FTP bandwidth handled by a SonicWALL appliance or group of SonicWALL appliances for the specified time period.

To view the FTP Usage Over Time report, follow these steps:

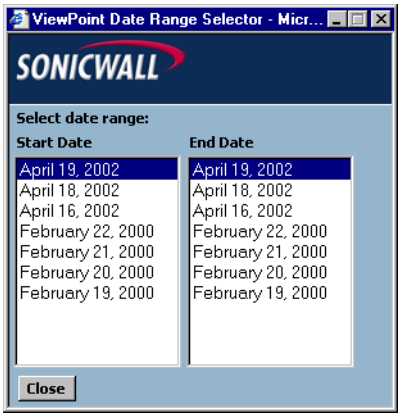
1. Start and log into ViewPoint.
2. Click the **Reports** tab.
3. Select the global icon, a group, or a SonicWALL appliance.
4. Expand the FTP Usage tree and click **Over Time**. The Over Time page appears (Figure 54).

Figure 54: Usage Over Time Page



5. The bar graph displays the amount of FTP bandwidth transferred during each day of the specified time period.
6. The table contains the following information:
   - **Date**—when the sample was taken.
   - **Connections**—number of FTP connections.
   - **MBytes**—number of megabytes transferred.
   - **% of Usage**—percentage of megabytes transferred during this day, compared to the time period. For example, if 10,000 megabytes of FTP data was transferred during the time period and 2,500 megabytes of FTP data was transferred on one day, the **% of Usage** field will display 25%.
7. To change the date range of the report, click **Settings**. The Reporting Date Range Selector dialog box appears (Figure 55).

Figure 55: Report Settings Dialog Box



8. Select the starting and ending dates that you would like to view.
9. When you are finished, click **Close.** The GMS Reporting Module displays the report for the selected date range.

   Note: *These settings will stay in effect for all reports during your active login session.*

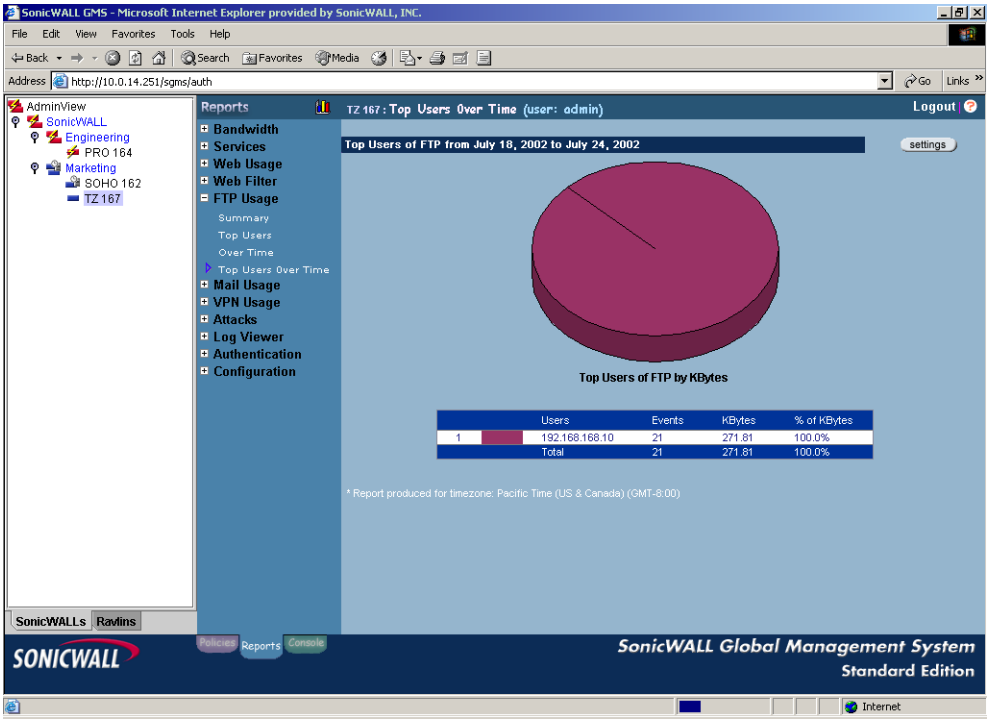
Viewing the Top Users of FTP Bandwidth Over Time

The Top Users Over Time report displays the users who used the most FTP bandwidth for the specified time period.

To view the Top Users Over Time report, follow these steps:

1. Start and log into ViewPoint.
2. Click the **Reports** tab.
3. Select a SonicWALL appliance.
4. Expand the FTP Usage tree and click **Top Users Over Time**. The Top Users Over Time page appears (Figure 56).

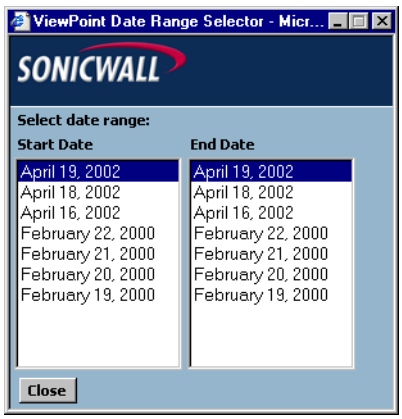
Figure 56: Top Users Over Time Page



5. The pie chart displays the percentage of bandwidth used by each user.

6. The table contains the following information:
   - **Users**—the IP address of the user.
   - **Events**—number of FTP Events.
   - **KBytes**—number of kilobytes transferred.
   - **% of KBytes**—percentage of kilobytes transferred by this user, compared to all users. For example, if 10000 kilobytes of data was transferred during the period and 2000 kilobytes was transferred by the top user, the **% of KBytes** field will display 20%.
7. To change the date range of the report, click **Settings**. The Reporting Date Range Selector dialog box appears (Figure 57).

   Figure 57: Report Settings Dialog Box



8. Select the starting and ending dates that you would like to view.
9. When you are finished, click **Close.** The GMS Reporting Module displays the report for the selected date range.

   Note: *These settings will stay in effect for all reports during your active login session.*

Viewing Mail Usage Reports

Mail usage reports provide information on the amount of mail usage that occurs through the selected SonicWALL appliance(s).

Mail usage reports can be used to view mail bandwidth usage by the hour, day, or over a period of days. Additionally, you can view the top users of mail bandwidth.

Note: *Mail usage reports include SMTP, POP3, and IMAP traffic.*

General bandwidth reports do not always provide a complete picture of network bandwidth usage. If a large amount of mail traffic occurs during peak times, you might want to take some of the following actions:

- Add bandwidth
- Upgrade network equipment
- Ask employees to use compression or transfer large files during non-peak times
- Ask employees to place large files on an FTP site rather than sending them as mail attachments.

Note: *All reports appear in Universal Time, Coordinated (UTC) or Greenwich Mean Time (GMT).*

Select from the following:

- To view a summary of the daily mail usage, see “Viewing the Mail Usage Summary Report” on page 57.
- To view the users who consume the most mail bandwidth, see “Viewing the Top Users of Mail Bandwidth” on page 59.
- To view mail usage over a period of time, see “Viewing Mail Usage Over Time” on page 60.
- To view the users who consume the most mail bandwidth over time, see “Viewing the Top Users of Mail Bandwidth Over Time” on page 62.

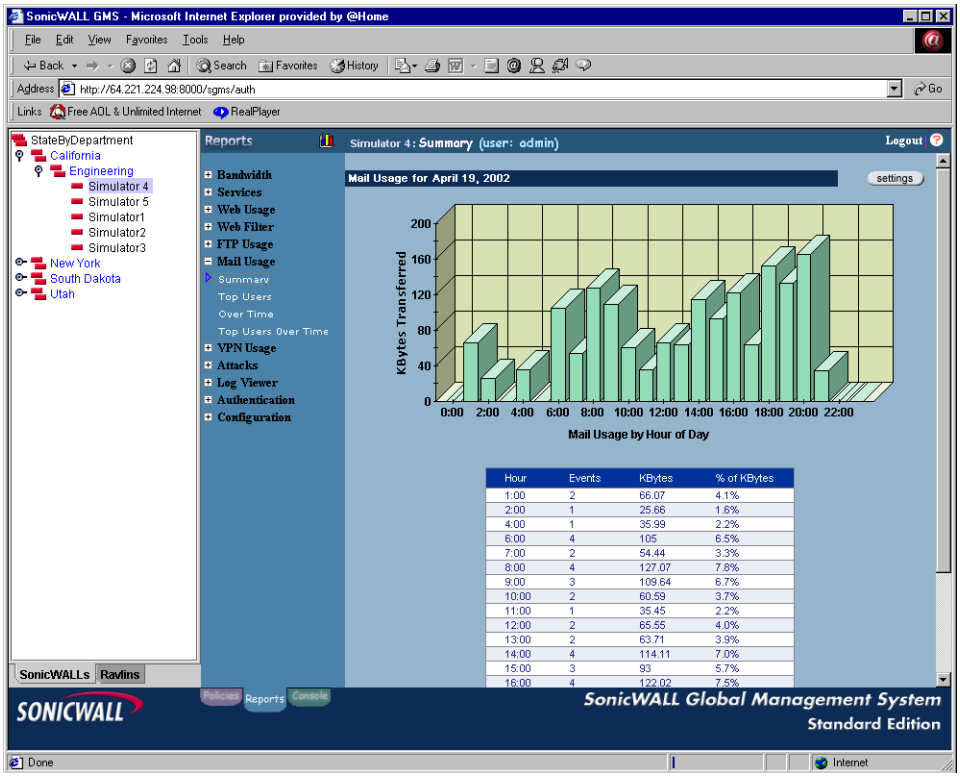
Viewing the Mail Usage Summary Report

The Mail Usage Summary report contains information on the amount of mail handled by a SonicWALL appliance or group of SonicWALL appliances during the specified day.

To view the Mail Usage Summary report, follow these steps:

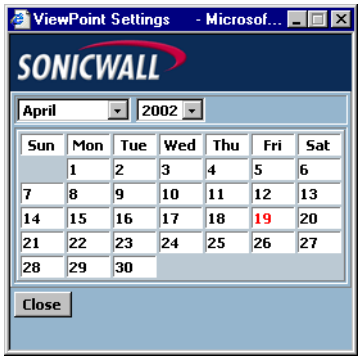
1. Start and log into ViewPoint.
2. Click the **Reports** tab.
3. Select the global icon, a group, or a SonicWALL appliance.
4. Expand the Mail Usage tree and click **Summary**. The Summary page appears (Figure 58).

Figure 58: Summary Page



5. The bar graph displays the amount of mail sent and received during each hour of the day.
6. The table contains the following information:
   - **Hour**—when the sample was taken.
   - **Events**—number of mail events.
   - **KBytes**—number of kilobytes transferred.
   - **% of KBytes**—percentage of kilobytes transferred during this hour, compared to the day. For example, if 10,000 kilobytes of mail was transferred during the day and 1,000 kilobytes was transferred at the 12:00 time period, the **% of KBytes** field will display 10%.
7. The GMS Reporting Module shows today's report. To change the date of the report, click **Settings**. The Report Settings dialog box appears (Figure 59).

Figure 59: Report Settings Dialog Box


ViewPoint Settings - Microsof...
SONICWALL
April
2002
Sun Mon Tue Wed Thu Fri Sat
1 2 3 4 5 6
7 8 9 10 11 12 13
14 15 16 17 18 19 20
21 22 23 24 25 26 27
28 29 30
Close

8. Select the year, month, and day that you would like to view.
9. When you are finished, click **Close.** The GMS Reporting Module displays the report for the selected day.

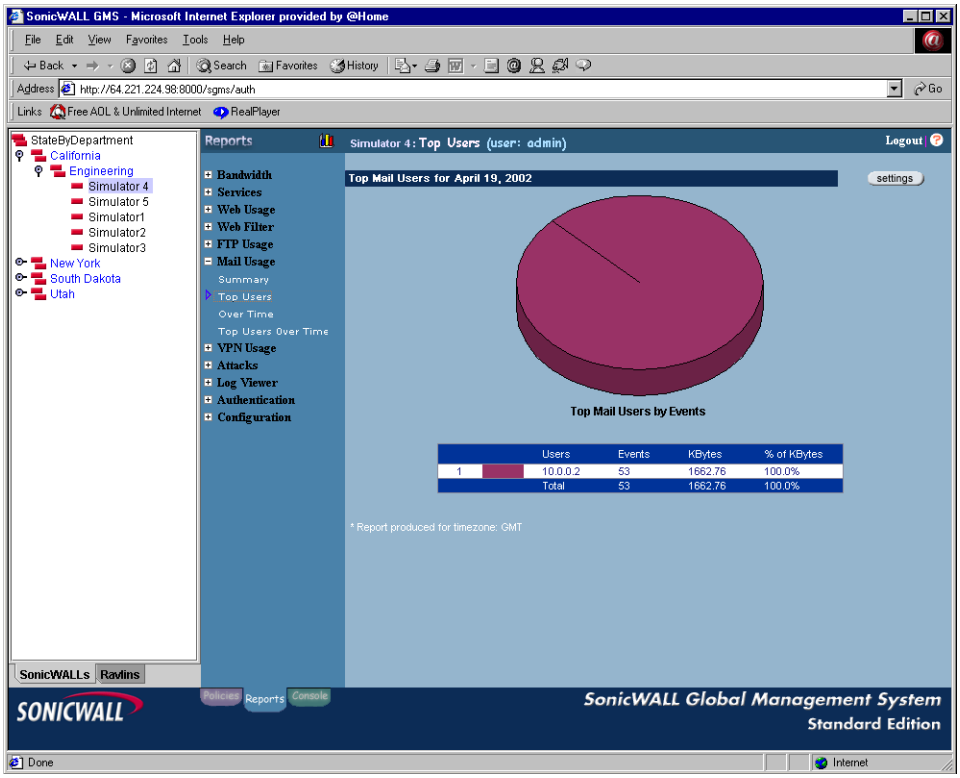
Viewing the Top Users of Mail Bandwidth

The Top Users report displays the users who sent and received the most mail on the specified date.

To view the Top Users report, follow these steps:

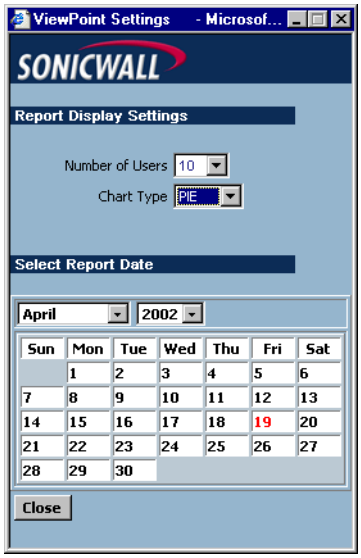
1. Start and log into ViewPoint.
2. Click the **Reports** tab.
3. Select a SonicWALL appliance.
4. Expand the Mail Usage tree and click **Top Users**. The Top Users page appears (Figure 60).

Figure 60: Top Users Page



5. The pie chart displays the percentage of mail sent and received by the top mail users.
6. The table contains the following information:
   - **Users**—the IP address of the user.
   - **Events**—number of mail messages sent and received.
   - **KBytes**—number of kilobytes transferred.
   - **% of KBytes**—percentage of kilobytes transferred by this user, compared to all users. For example, if 10000 kilobytes of data was transferred during the day and 2000 kilobytes was transferred by the top user, the **% of KBytes** field will display 20%.
7. By default, the GMS Reporting Module shows today's report, a pie chart, and the ten top users. To change these settings, click **Settings**. The Report Settings dialog box appears (Figure 61).

Figure 61: Report Settings Dialog Box


ViewPoint Settings - Microsof...
SONICWALL
Report Display Settings
Number of Users 10
Chart Type PIE
Select Report Date
April 2002
Sun Mon Tue Wed Thu Fri Sat
1 2 3 4 5 6
7 8 9 10 11 12 13
14 15 16 17 18 19 20
21 22 23 24 25 26 27
28 29 30
Close

8. Select the number of users that will be displayed from the **Number of Users** list box.
9. Select the type of chart from the **Chart Type** list box.
10. Select the year, month, and day that you would like to view.
11. When you are finished, click **Close.** The GMS Reporting Module displays the report for the selected day.

    Note: *These settings will stay in effect for all reports during your active login session.*

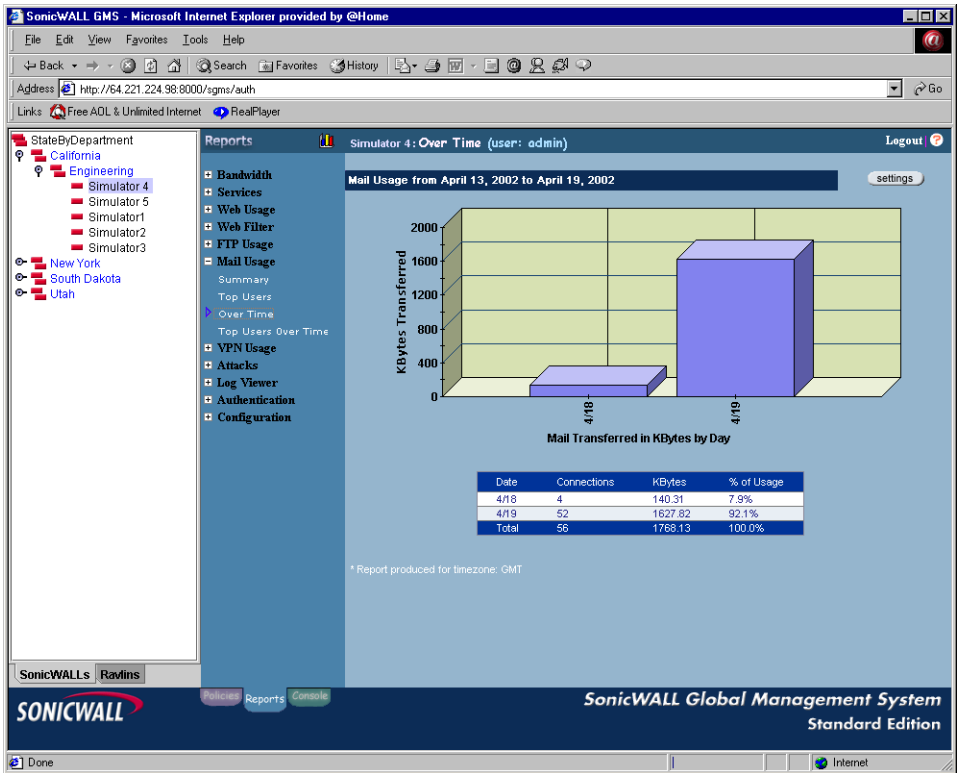
Viewing Mail Usage Over Time

The Mail Usage Over Time report displays the daily amount of mail handled by a SonicWALL appliance or group of SonicWALL appliances for the specified time period.

To view the Mail Usage Over Time report, follow these steps:

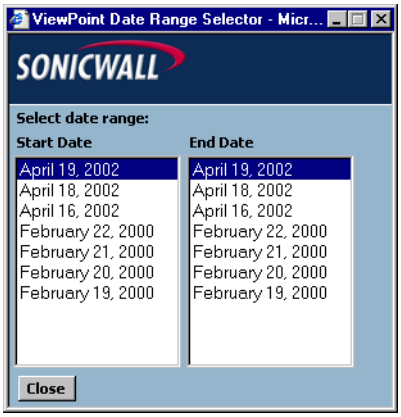
1. Start and log into ViewPoint.
2. Click the **Reports** tab.
3. Select the global icon, a group, or a SonicWALL appliance.
4. Expand the Mail Usage tree and click **Over Time**. The Over Time page appears (Figure 62).

Figure 62: Over Time Page



5. The bar graph displays the amount of mail sent and received during each day of the specified time period.
6. The table contains the following information:
   - **Date**—when the sample was taken.
   - **Connections**—number of mail messages.
   - **KBytes**—number of kilobytes transferred.
   - **% of Usage**—percentage of kilobytes transferred during this day, compared to the time period. For example, if 10,000 kilobytes of mail was transferred during the time period and 2,500 kilobytes of mail was transferred on one day, the **% of Usage** field will display 25%.
7. To change the date range of the report, click **Settings**. The Reporting Date Range Selector dialog box appears (Figure 63).

Figure 63: Report Settings Dialog Box



8. Select the starting and ending dates that you would like to view.
9. When you are finished, click **Close.** The GMS Reporting Module displays the report for the selected date range.

   Note: *These settings will stay in effect for all reports during your active login session.*

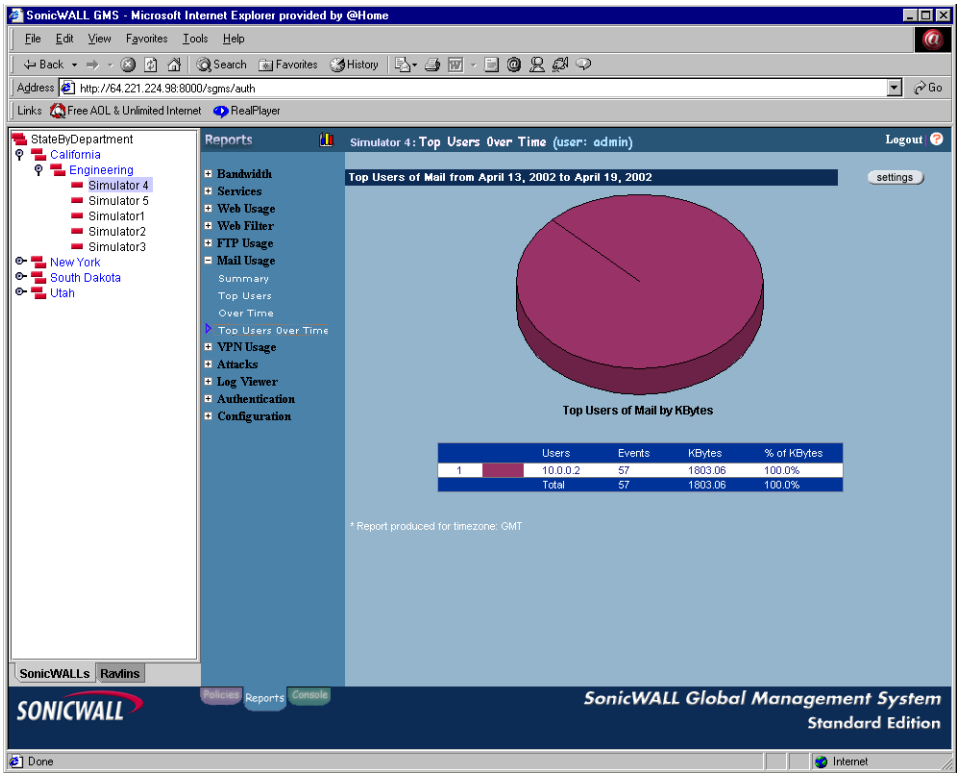
Viewing the Top Users of Mail Bandwidth Over Time

The Top Users Over Time report displays the users who sent and received the most mail during the specified time period.

To view the Top Users Over Time report, follow these steps:

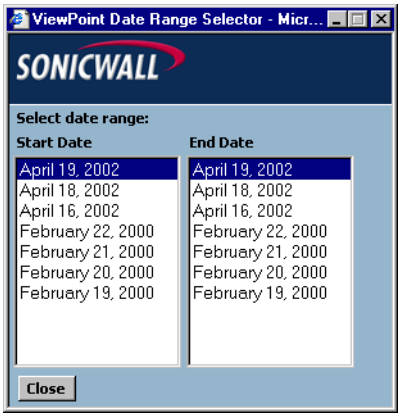
1. Start and log into ViewPoint.
2. Click the **Reports** tab.
3. Select a SonicWALL appliance.
4. Expand the Mail Usage tree and click **Top Users Over Time**. The Top Users Over Time page appears (Figure 64).

Figure 64: Top Users Over Time Page



5. The pie chart displays the percentage of mail sent and received by the top mail users.
6. The table contains the following information:
   - **Users**—the IP address of the user.
   - **Events**—number of mail messages sent and received.
   - **KBytes**—number of kilobytes transferred.
   - **% of KBytes**—percentage of kilobytes transferred by this user, compared to all users. For example, if 10000 kilobytes of data was transferred during the period and 2000 kilobytes was transferred by the top user, the **% of KBytes** field will display 20%.
7. To change the date range of the report, click **Settings**. The Reporting Date Range Selector dialog box appears (Figure 65).

Figure 65: Report Settings Dialog Box



8. Select the starting and ending dates that you would like to view.
9. When you are finished, click **Close**.GMS Reporting displays the report for the selected date range.

   Note: *These settings will stay in effect for all reports during your active login session.*

Viewing VPN Usage Reports

VPN Usage reports provide information on the amount of VPN usage that occurs through the selected SonicWALL appliance(s).

VPN Usage reports can be used to view VPN usage by the hour, day, or over a period of days. Additionally, you can view the top users of VPN.

General bandwidth reports do not always provide a complete picture of network bandwidth usage. If a large amount of VPN traffic occurs, you might need to add bandwidth, upgrade network equipment, or reconfigure the VPN network.

Note: *All reports appear in Universal Time, Coordinated (UTC) or Greenwich Mean Time (GMT).*

Select from the following:

- To view a summary of the daily VPN bandwidth usage, see "Viewing the VPN Usage Summary Report" on page 64.
- To view the users who consume the most VPN bandwidth, see "Viewing the Top VPN Users" on page 65.
- To view VPN bandwidth usage over a period of time, see "Viewing VPN Usage Over Time" on page 67.
- To view the users who consume the most VPN bandwidth over time, see "Viewing VPN Usage Over Time" on page 67.

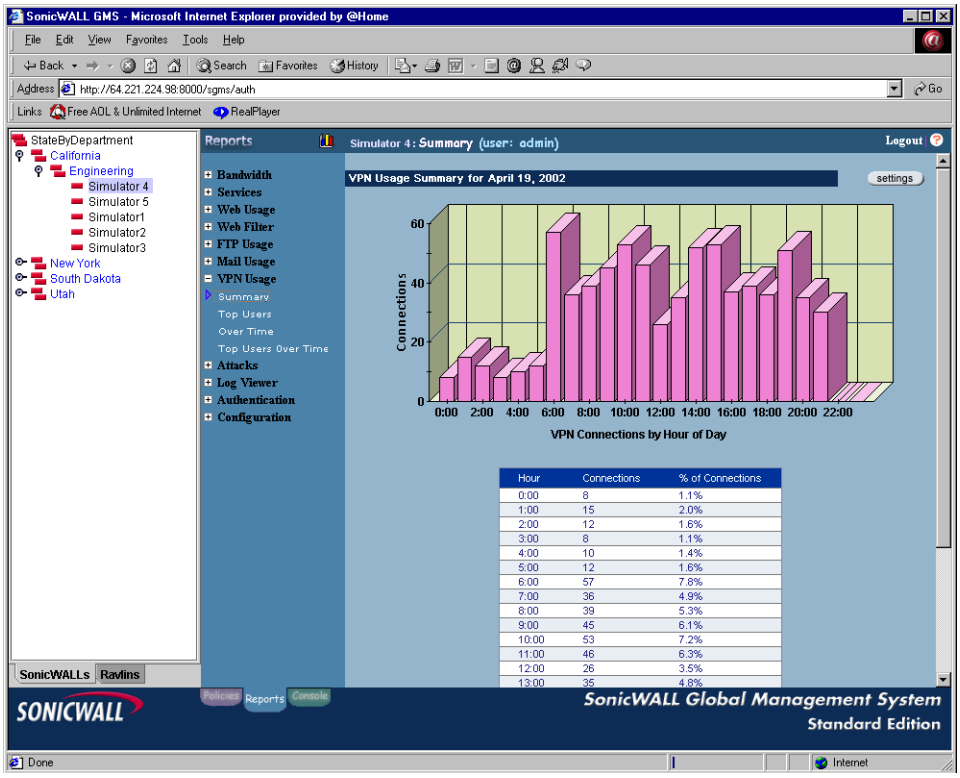
Viewing the VPN Usage Summary Report

The VPN Usage Summary report contains information on the number of VPN connections made through a SonicWALL appliance or group of SonicWALL appliances during the specified day.

To view the VPN Usage Summary report, follow these steps:

1. Start and log into ViewPoint.
2. Click the **Reports** tab.
3. Select the global icon, a group, or a SonicWALL appliance.
4. Expand the VPN Usage tree and click **Summary**. The Summary page appears (Figure 66).

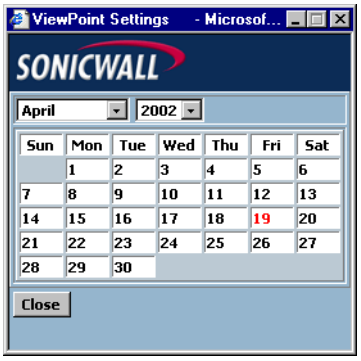
Figure 66: Summary Page


SonicWALL GMS - Microsoft Internet Explorer provided by @Home
Simulator 4 : Summary (user: admin)
Logout
VPN Usage Summary for April 19, 2002
settings
Connections
VPN Connections by Hour of Day
Hour Connections % of Connections
SonicWALL Global Management System
Standard Edition

5. The bar graph displays the number of VPN connections made during each hour of the day.

6. The table contains the following information:
   - **Hour**—when the sample was taken.
   - **Connections**—number of VPN connections.
   - **% of Connections**—percentage of VPN connections during this hour, compared to the day. For example, if 10,000 connections occurred during the day and 1,000 connections occurred during the 2:00 time period, the **% of Connections** field will display 10%.
7. The GMS Reporting Module shows today's report. To change the date of the report, click **Settings**. The Report Settings dialog box appears (Figure 67).

Figure 67: Report Settings Dialog Box


ViewPoint Settings - Microsof...
SONICWALL
April
2002
Sun Mon Tue Wed Thu Fri Sat
1 2 3 4 5 6
7 8 9 10 11 12 13
14 15 16 17 18 19 20
21 22 23 24 25 26 27
28 29 30
Close

8. Select the year, month, and day that you would like to view.
9. When you are finished, click **Close.** The GMS Reporting Module displays the report for the selected day.

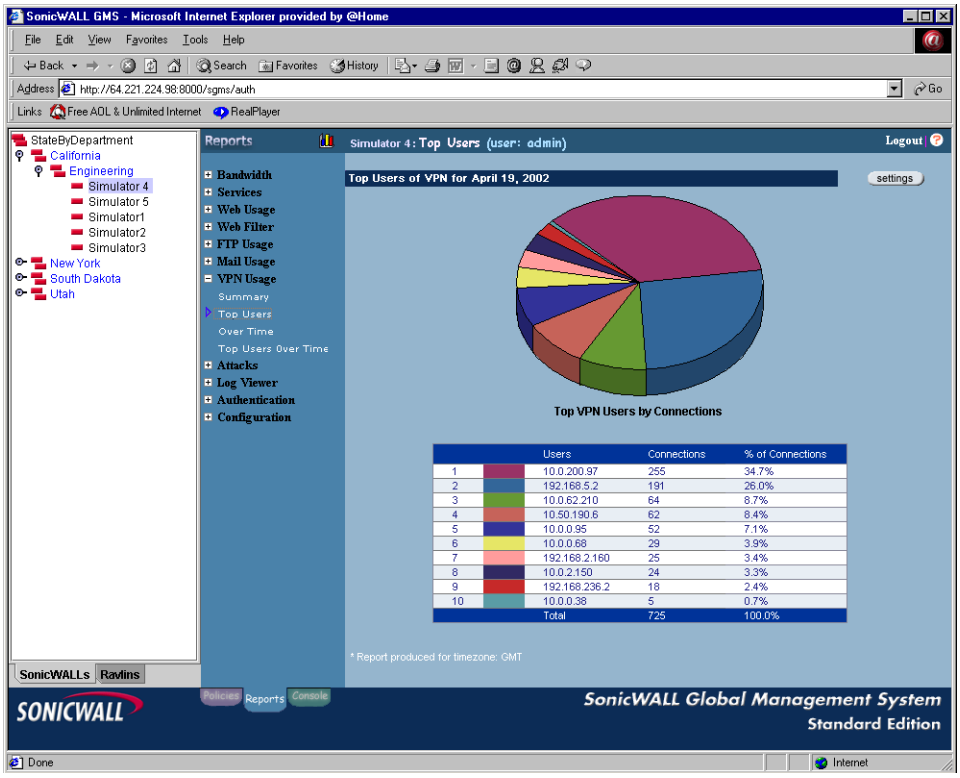
Viewing the Top VPN Users

The Top Users report displays the users who made the most VPN connections on the specified date.

To view the Top Users report, follow these steps:

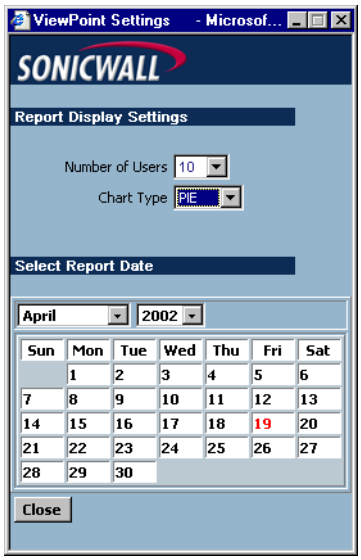
1. Start and log into ViewPoint.
2. Click the **Reports** tab.
3. Select a SonicWALL appliance.
4. Expand the VPN Usage tree and click **Top Users**. The Top Users page appears (Figure 68).

Figure 68: Top Users Page



5. The pie chart displays the VPN connections for the top VPN users.
6. The table contains the following information:
   - **Users**—the IP address of the user.
   - **Connections**—number of VPN connections.
   - **% of Connections**—percentage of VPN connections made by this user, compared to all other users. For example, if 10,000 connections occurred during the day and 1,000 connections were made by one user, the **% of Connections** field will display 10%.
7. By default, the GMS Reporting Module shows today's report, a pie chart, and the ten top users. To change these settings, click **Settings**. The Report Settings dialog box appears (Figure 69).

Figure 69: Report Settings Dialog Box


ViewPoint Settings - Microsof...
SONICWALL
Report Display Settings
Number of Users 10
Chart Type PIE
Select Report Date
April 2002
Sun Mon Tue Wed Thu Fri Sat
1 2 3 4 5 6
7 8 9 10 11 12 13
14 15 16 17 18 19 20
21 22 23 24 25 26 27
28 29 30
Close

8. Select the number of users that will be displayed from the **Number of Users** list box.

9. Select the type of chart from the **Chart Type** list box.
10. Select the year, month, and day that you would like to view.
11. When you are finished, click **Close.** The GMS Reporting Module displays the report for the selected day.

    Note: *These settings will stay in effect for all reports during your active login session.*

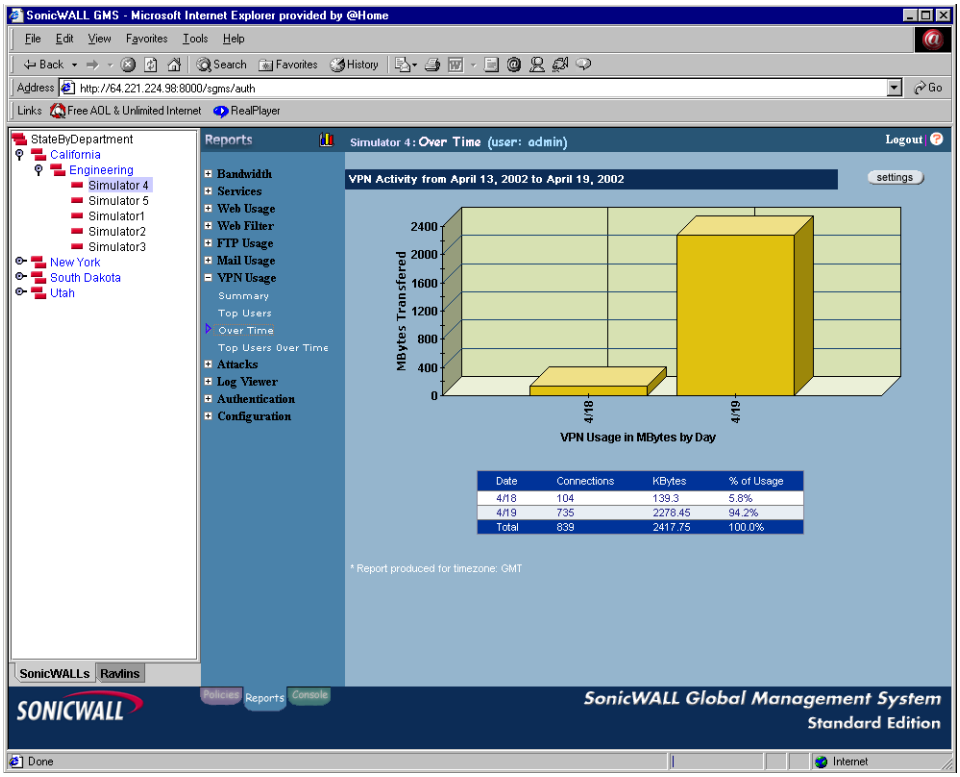
Viewing VPN Usage Over Time

The VPN Usage Over Time report displays the daily number of VPN connections made through a SonicWALL appliance or group of SonicWALL appliances during the specified time period.

To view the VPN Usage Over Time report, follow these steps:

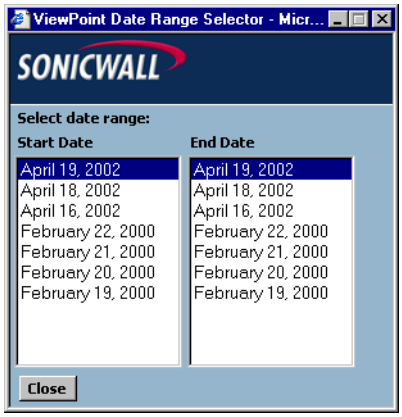
1. Start and log into ViewPoint.
2. Click the **Reports** tab.
3. Select the global icon, a group, or a SonicWALL appliance.
4. Expand the VPN Usage tree and click **Over Time**. The Over Time page appears (Figure 70).

Figure 70: Over Time Page



5. The bar graph displays the number of VPN connections made during each day of the specified time period.
6. The table contains the following information:
   - **Date**—when the sample was taken.
   - **Connections**—number of connections.
   - **KBytes**—number of kilobytes transferred.
   - **% of Usage**—percentage of kilobytes transferred during this day, compared to the time period. For example, if 10,000 kilobytes of mail was transferred during the time period and 2,500 kilobytes of mail was transferred on one day, the **% of Usage** field will display 25%.
7. To change the date range of the report, click **Settings**. The Reporting Date Range Selector dialog box appears (Figure 71).

Figure 71: Report Settings Dialog Box



8. Select the starting and ending dates that you would like to view.
9. When you are finished, click **Close.** The GMS Reporting Module displays the report for the selected date range.

   Note: *These settings will stay in effect for all reports during your active login session.*

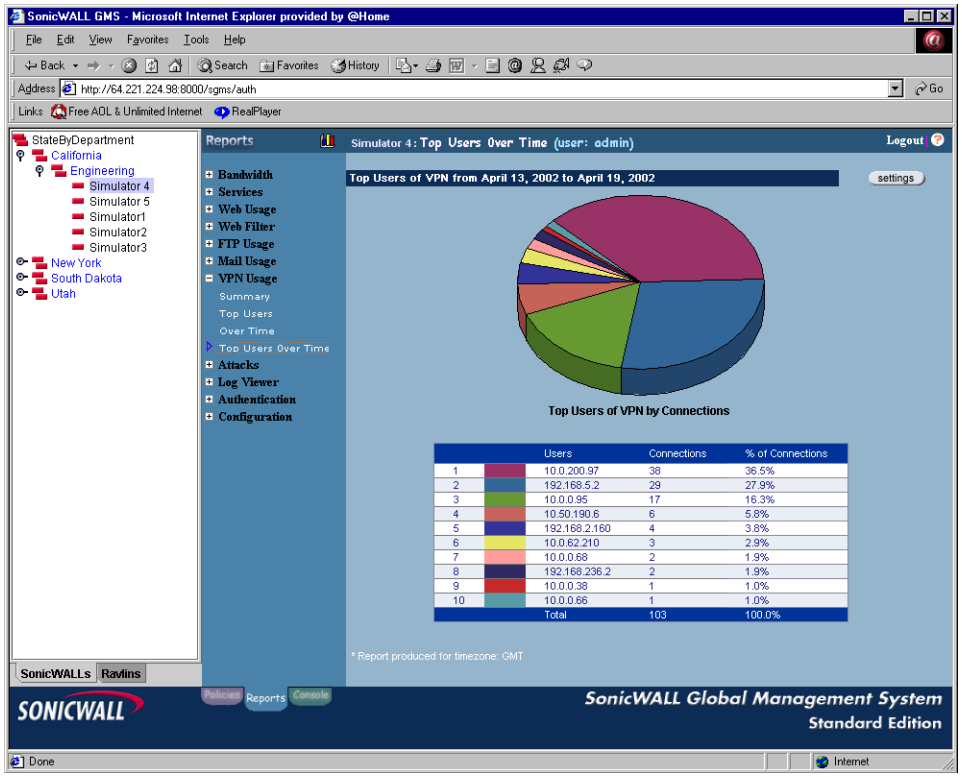
Viewing the Top VPN Users Over Time

The Top Users report displays the users who made the most VPN connections for the specified time period.

To view the Top Users report, follow these steps:

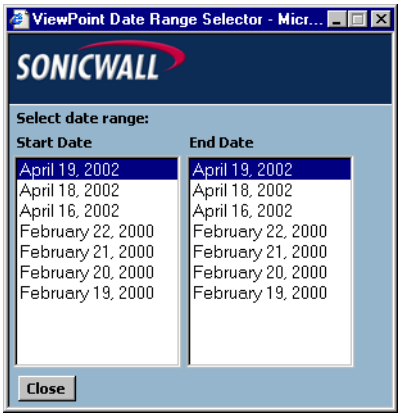
1. Start and log into ViewPoint.
2. Click the **Reports** tab.
3. Select a SonicWALL appliance.
4. Expand the VPN Usage tree and click **Top Users Over Time**. The Top Users Over Time page appears (Figure 72).

Figure 72: Top Users Over Time Page



5. The pie chart displays the VPN connections for the top VPN users.
6. The table contains the following information:
   - **Users**—the IP address of the user.
   - **Connections**—number of VPN connections.
   - **% of Connections**—percentage of VPN connections made by this user, compared to all other users. For example, if 10,000 connections occurred during the period and 1,000 connections were made by one user, the **% of Connections** field will display 10%.
7. To change the date range of the report, click **Settings**. The Reporting Date Range Selector dialog box appears (Figure 73).

   Figure 73: Report Settings Dialog Box



8. Select the starting and ending dates that you would like to view.
9. When you are finished, click **Close.** The GMS Reporting Module displays the report for the selected date range.

   Note: *These settings will stay in effect for all reports during your active login session.*

Viewing Attack Reports

Attack reports show the number of attacks that were directed at or through the selected SonicWALL appliance(s). These include denial of service attacks, intrusions, probes, and all other malicious activity directed at the SonicWALL appliance or computers on the LAN or DMZ.

Note: *All reports appear in Universal Time, Coordinated (UTC) or Greenwich Mean Time (GMT).*

Select from the following:

- To view a summary of the attacks, see "Viewing the Attack Summary Report" on page 70.
- To view the attacks by attack category, see "Viewing the Attacks by Category" on page 71.
- To view the attacks by source IP address, see "Viewing the Attacks by Source" on page 73.
- To view a summary of the errors and exceptions, see "Viewing the Errors and Exceptions Report" on page 74.
- To view attacks over a period of time, see "Viewing Attack Reports Over Time" on page 76.
- To view errors and exceptions over a period of time, see "Viewing Errors Over Time" on page 77.

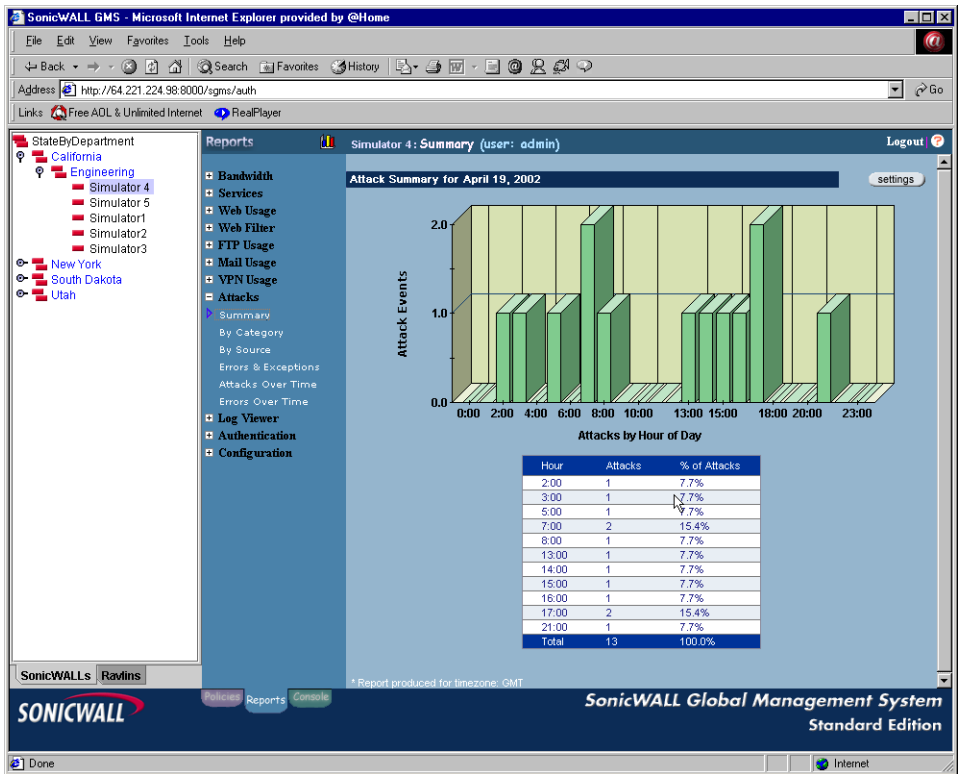
Viewing the Attack Summary Report

The Attack Summary report contains information on the number of attacks attempted on a SonicWALL appliance or group of SonicWALL appliances during the specified day.

To view the Attack Summary report, follow these steps:

1. Start and log into ViewPoint.
2. Click the **Reports** tab.
3. Select the global icon, a group, or a SonicWALL appliance.
4. Expand the Attacks tree and click **Summary**. The Summary page appears (Figure 74).

Figure 74: Summary Page

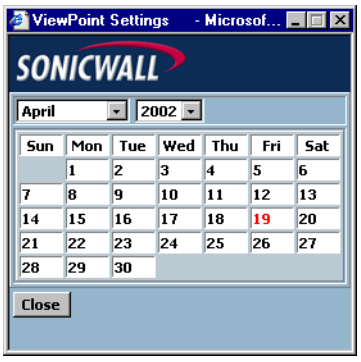


5. The bar graph displays the number of attacks attempted during each hour of the day. The table contains the following information:
   - **Hour**—when the sample was taken.
   - **Attacks**—number of attack attempts.

- **% of Attacks**—percentage of attacks during this hour, compared to the day. For example, if 1,000 attacks occurred during the day and 100 attacks occurred during the 2:00 time period, the **% of Attacks** field will display 10%.

6. The GMS Reporting Module shows today's report. To change the date of the report, click **Settings**. The Report Settings dialog box appears (Figure 75).

Figure 75: Report Settings Dialog Box


ViewPoint Settings - Microsof...
SONICWALL
April
2002
Sun Mon Tue Wed Thu Fri Sat
1 2 3 4 5 6
7 8 9 10 11 12 13
14 15 16 17 18 19 20
21 22 23 24 25 26 27
28 29 30
Close

7. Select the year, month, and day that you would like to view.
8. When you are finished, click **Close.** The GMS Reporting Module displays the report for the selected day.

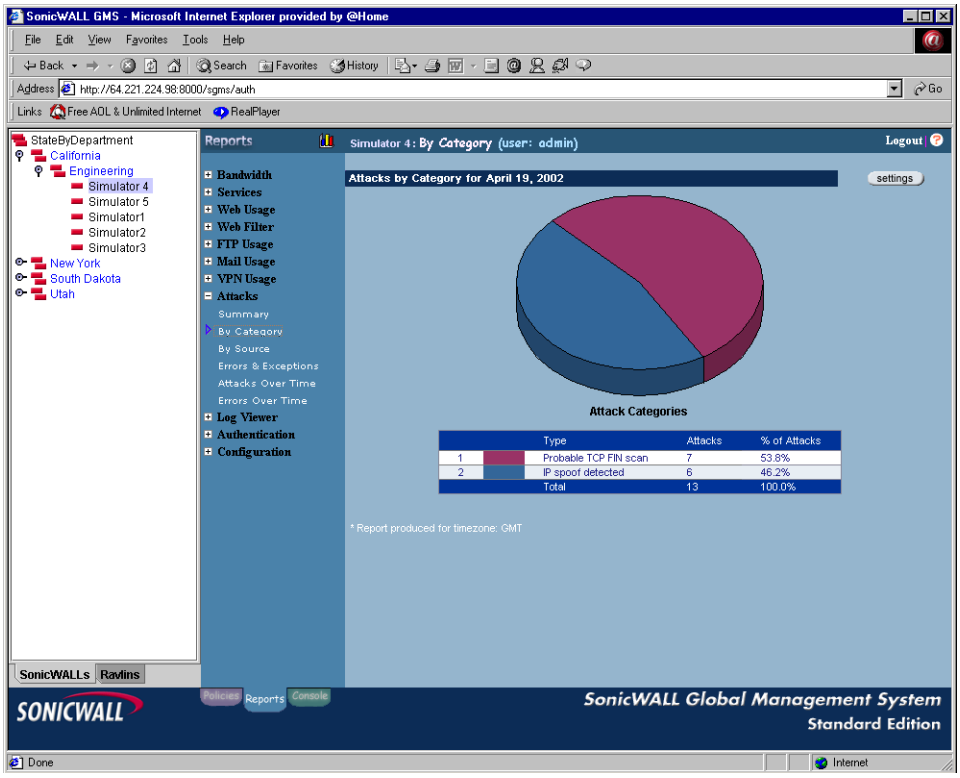
Viewing the Attacks by Category

The Attacks by Category report displays the attacks that occurred on the specified date, sorted by category.

To view the Attacks by Category report, follow these steps:

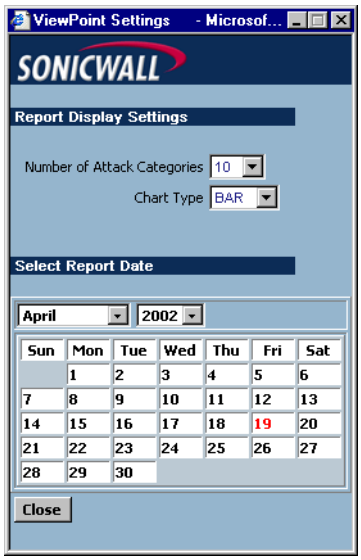
1. Start and log into ViewPoint.
2. Click the **Reports** tab.
3. Select a SonicWALL appliance.
4. Expand the Attacks tree and click **By Category**. The By Category page appears (Figure 76).

Figure 76: By Category Page



5. The pie chart displays the percentage of each type of attack.
6. The table contains the following information:
   - **Type**—the type of attack.
   - **Attacks**—number of attacks.
   - **% of Attacks**—percentage of this type of attack, compared to all other attack types. For example, if 5,000 attacks occurred during the day and the IP Spoof makes up 500 of the attacks, its **% of Attacks** field will display 10%.
7. By default, the GMS Reporting Module shows today's report, a pie chart, and the ten top categories. To change these settings, click **Settings**. The Report Settings dialog box appears (Figure 77).

Figure 77: Report Settings Dialog Box


ViewPoint Settings - Microsof...
SONICWALL
Report Display Settings
Number of Attack Categories 10
Chart Type BAR
Select Report Date
April 2002
Sun Mon Tue Wed Thu Fri Sat
1 2 3 4 5 6
7 8 9 10 11 12 13
14 15 16 17 18 19 20
21 22 23 24 25 26 27
28 29 30
Close

8. Select the number of categories that will be displayed from the **Number of Categories** list box.

9. Select the type of chart from the **Chart Type** list box.
10. Select the year, month, and day that you would like to view.
11. When you are finished, click **Close.** The GMS Reporting Module displays the report for the selected day.

    Note: *These settings will stay in effect for all reports during your active login session.*

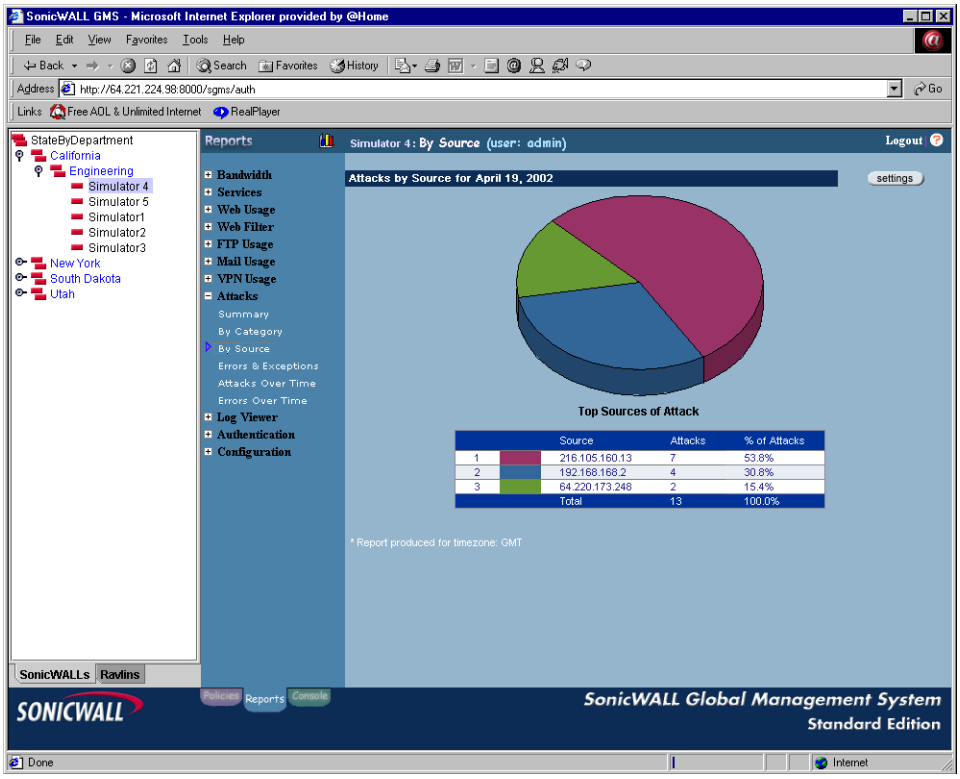
Viewing the Attacks by Source

The Attacks by Source report displays the top sources of attacks.

To view the Attacks by Source report, follow these steps:

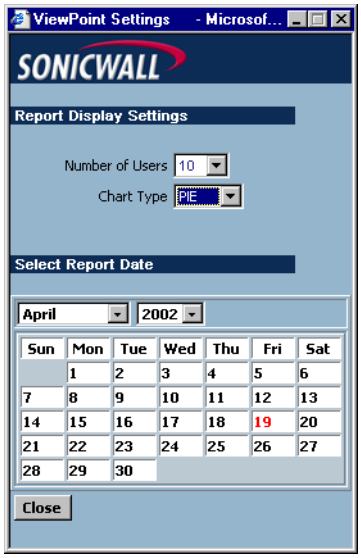
1. Start and log into ViewPoint.
2. Click the **Reports** tab.
3. Select a SonicWALL appliance.
4. Expand the Attacks tree and click **By Source**. The By Source page appears (Figure 78).

Figure 78: By Source Page



5. The pie chart displays the percentage of each source of attack.
6. The table contains the following information:
   - **Source**—the source of the attack.
   - **Attacks**—number of attacks.
   - **% of Attacks**—percentage of attacks from this source, compared to all other sources. For example, if 1,000 attacks occurred during the day and 500 attacks came from one source, its **% of Attacks** field will display 50%.
7. By default, the GMS Reporting Module shows today's report, a pie chart, and the ten top sources. To change these settings, click **Settings**. The Report Settings dialog box appears (Figure 79).

Figure 79: Report Settings Dialog Box


ViewPoint Settings - Microsof...
SONICWALL
Report Display Settings
Number of Users 10
Chart Type PIE
Select Report Date
April 2002
Sun Mon Tue Wed Thu Fri Sat
1 2 3 4 5 6
7 8 9 10 11 12 13
14 15 16 17 18 19 20
21 22 23 24 25 26 27
28 29 30
Close

8. Select the number of sources that will be displayed from the **Number of Sources** list box.
9. Select the type of chart from the **Chart Type** list box.
10. Select the year, month, and day that you would like to view.
11. When you are finished, click **Close.** The GMS Reporting Module displays the report for the selected day.

    Note: *These settings will stay in effect for all reports during your active login session.*

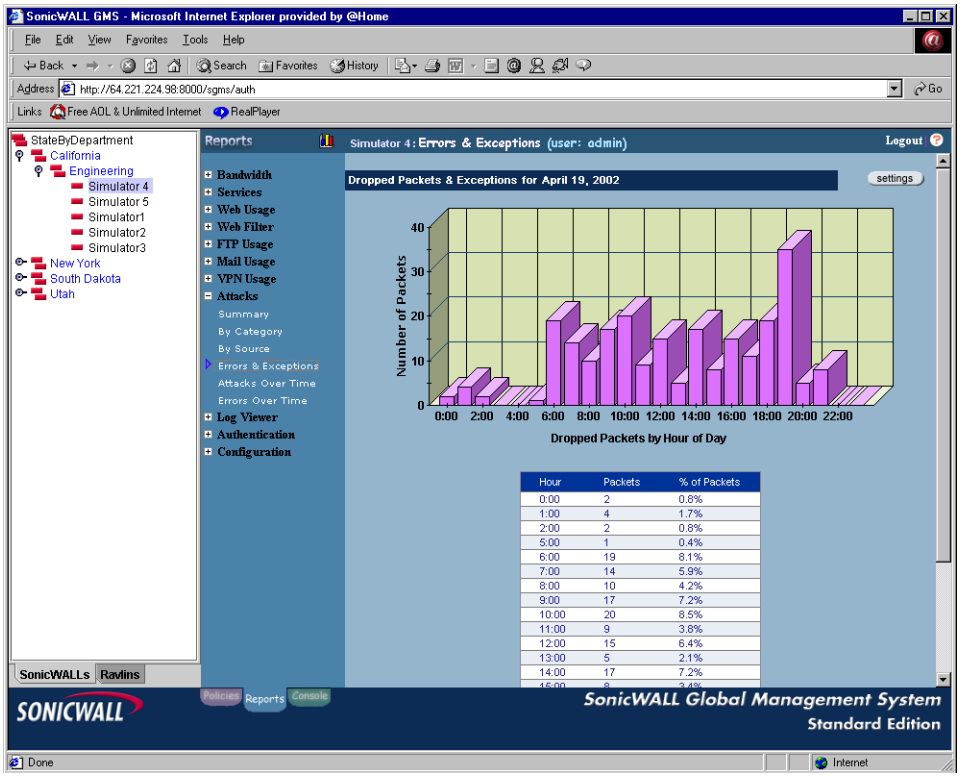
Viewing the Errors and Exceptions Report

The Errors and Exceptions Summary report contains information on the number of dropped packets on a SonicWALL appliance or group of SonicWALL appliances during the specified day.

To view the Errors and Exceptions report, follow these steps:

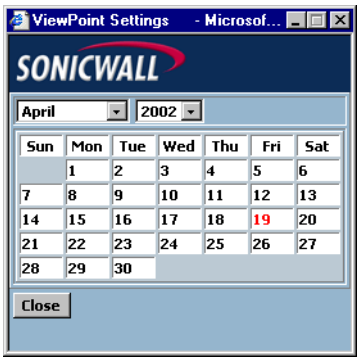
1. Start and log into ViewPoint.
2. Click the **Reports** tab.
3. Select the global icon, a group, or a SonicWALL appliance.
4. Expand the Attacks tree and click **Errors & Exceptions**. The Errors & Exceptions page appears (Figure 74).

Figure 80: Errors & Exceptions Page



5. The bar graph displays the packets that were dropped during each hour of the day.
6. The table contains the following information:
   - **Hour**—when the sample was taken.
   - **Packets**—number of dropped packets.
   - **% of Packets**—percentage of packets dropped during this hour, compared to the day. For example, if 1,000 packets were dropped during the day and 100 packets were dropped during the 1:00 time period, the **% of Packets** field will display 10%.
7. The GMS Reporting Module shows today's report. To change the date of the report, click **Settings**. The Report Settings dialog box appears (Figure 81).

Figure 81: Report Settings Dialog Box


ViewPoint Settings - Microsof...
SONICWALL
April
2002
Sun Mon Tue Wed Thu Fri Sat
1 2 3 4 5 6
7 8 9 10 11 12 13
14 15 16 17 18 19 20
21 22 23 24 25 26 27
28 29 30
Close

8. Select the year, month, and day that you would like to view.
9. When you are finished, click **Close.** The GMS Reporting Module displays the report for the selected day.

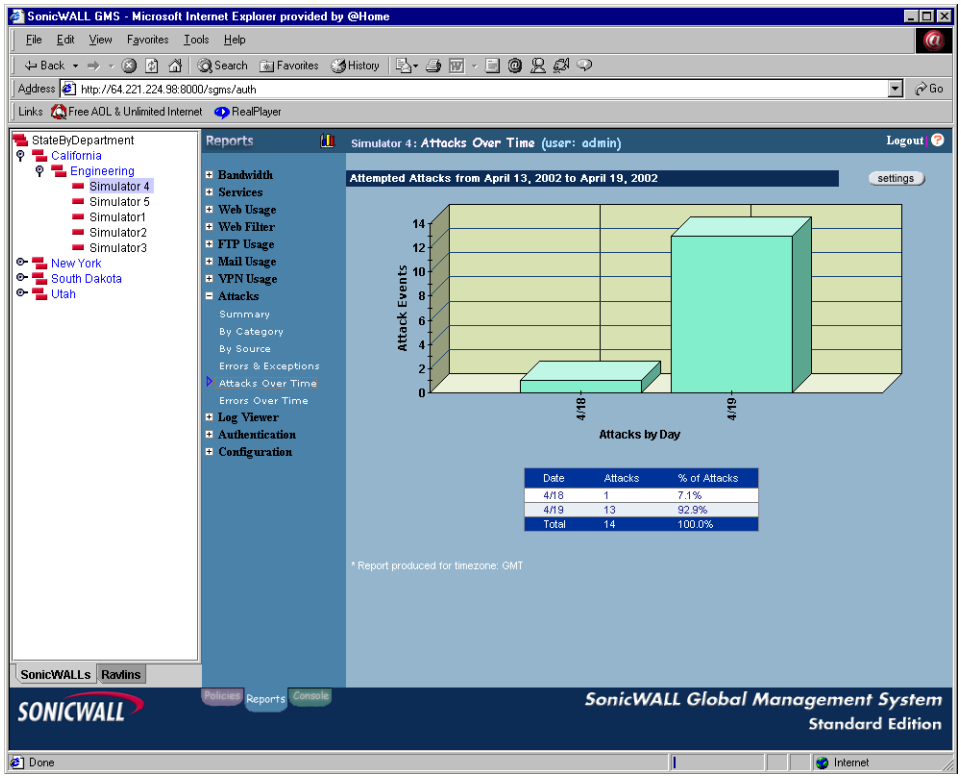
Viewing Attack Reports Over Time

The Attacks Over Time report displays the daily number of attempted attacks during the specified time period.

To view the Attacks Over Time report, follow these steps:

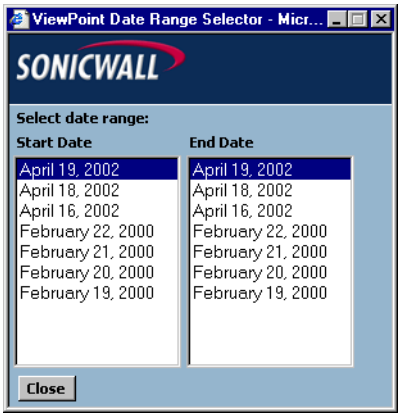
1. Start and log into ViewPoint.
2. Click the **Reports** tab.
3. Select the global icon, a group, or a SonicWALL appliance.
4. Expand the Attacks tree and click **Attacks Over Time**. The Attacks Over Time page appears (Figure 82).

Figure 82: Attacks Over Time Page



5. The bar graph displays the number of attacks attempted each day of the specified time period.
6. The table contains the following information:
   - **Date**—when the sample was taken.
   - **Attacks**—number of attacks.
   - **% of Attacks**—percentage of attacks on this day, compared to the time period. For example, if 10,000 attacks occurred during the time period and 1,000 attacks occurred on Thursday, its **% of Attacks** field will display 10%.
7. To change the date range of the report, click **Settings**. The Reporting Date Range Selector dialog box appears (Figure 83).

Figure 83: Report Settings Dialog Box



8. Select the starting and ending dates that you would like to view.
9. When you are finished, click **Close.** The GMS Reporting Module displays the report for the selected date range.

   Note: *These settings will stay in effect for all reports during your active login session.*

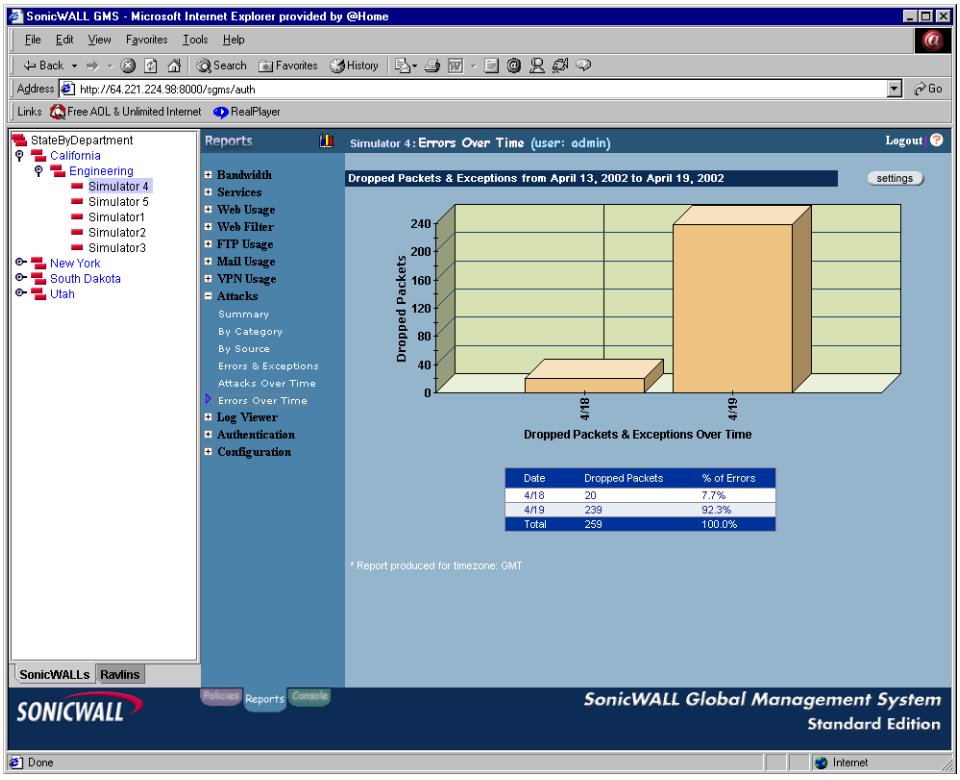
Viewing Errors Over Time

The Errors Over Time report displays the number of errors during the specified time period.

To view the Errors Over Time report, follow these steps:

1. Start and log into ViewPoint.
2. Click the **Reports** tab.
3. Select the global icon, a group, or a SonicWALL appliance.
4. Expand the Attacks tree and click **Errors Over Time**. The Errors Over Time page appears (Figure 84).

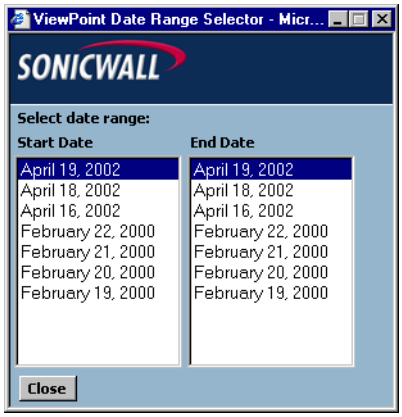
Figure 84: Errors Over Time Page



5. The bar graph displays the number of packets that were dropped during each day of the specified time period.

6. The table contains the following information:
   - **Date**—when the sample was taken.
   - **Dropped Packets**—number of dropped packets.
   - **% of Errors**—percentage of dropped packets on this day, compared to the time period. For example, if 10,000 packets were dropped during the time period and 1,000 packets were dropped on Wednesday, its **% of Attacks** field will display 10%.
7. To change the date range of the report, click **Settings**. The Reporting Date Range Selector dialog box appears (Figure 85).

   Figure 85: Report Settings Dialog Box



8. Select the starting and ending dates that you would like to view.
9. When you are finished, click **Close.** The GMS Reporting Module displays the report for the selected date range.

   Note: *These settings will stay in effect for all reports during your active login session.*

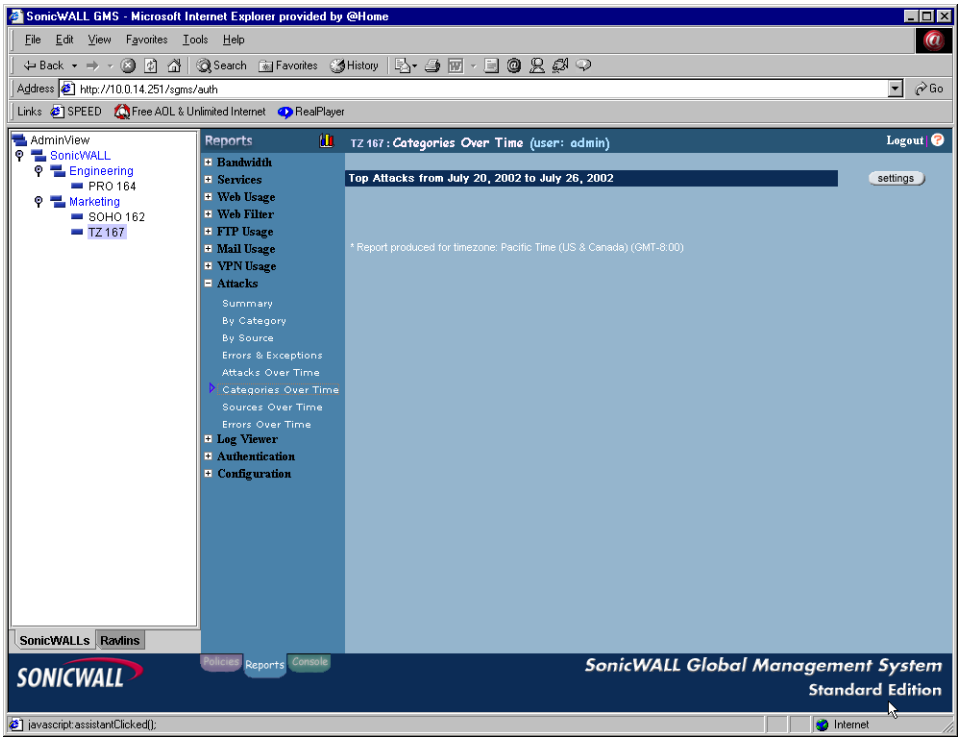
Categories Over Time

The Categories Over Time report displays the number of attacks in each attack category during the specified time period.

To view the Categories Over Time report, follow these steps:

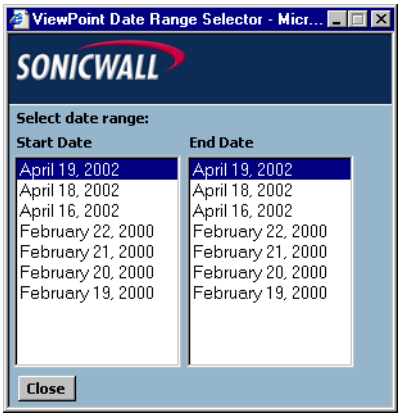
1. Start and log into ViewPoint.
2. Click the **Reports** tab.
3. Select the global icon, a group, or a SonicWALL appliance.
4. Expand the Attacks tree and click **Categories Over Time**. The Categories Over Time page appears (Figure 86).

Figure 86: Catagories Over Time Page



5. The bar graph displays the number of attacks attempted each day of the specified time period.
6. The table contains the following information:
   - **Category**—category of the attack.
   - **Attacks**—number of attacks.
   - **% of Attacks**—percentage of attacks for this category, compared to other categories. For example, if 5,000 attacks occurred during the time period and 1,000 attacks occurred for a category, its **% of Attacks** field will display 20%.
7. To change the date range of the report, click **Settings**. The Reporting Date Range Selector dialog box appears (Figure 87).

Figure 87: Report Settings Dialog Box



8. Select the starting and ending dates that you would like to view.
9. When you are finished, click **Close.** The GMS Reporting Module displays the report for the selected date range.

   Note: *These settings will stay in effect for all reports during your active login session.*

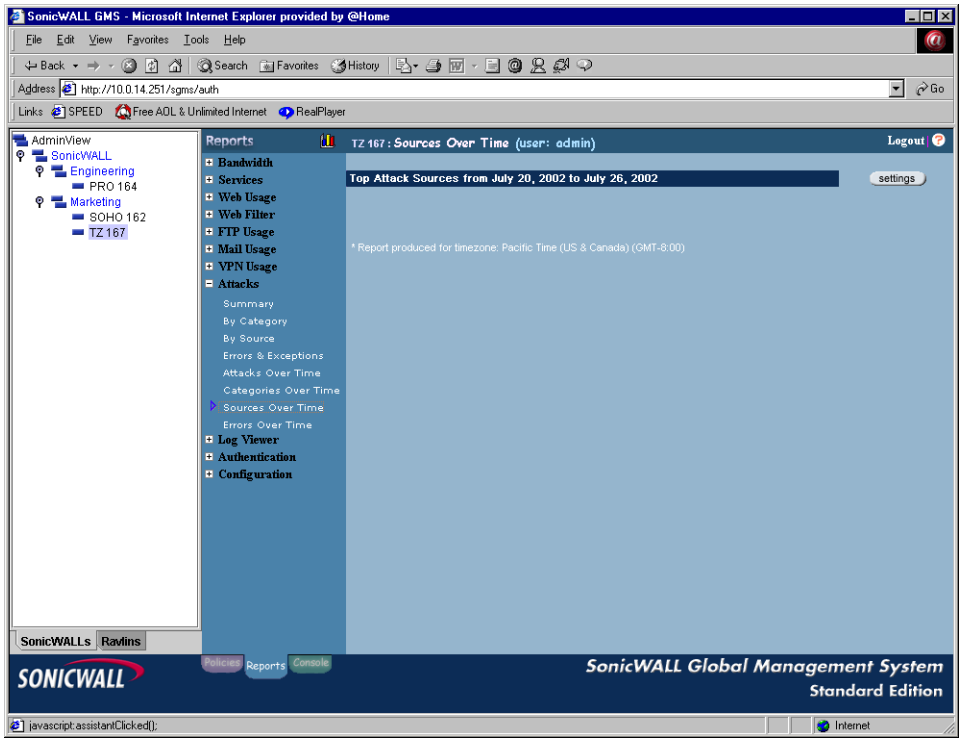
Sources Over Time

The Source Over Time report displays the number of attacks from each major source during the specified time period.

To view the Sources Over Time report, follow these steps:

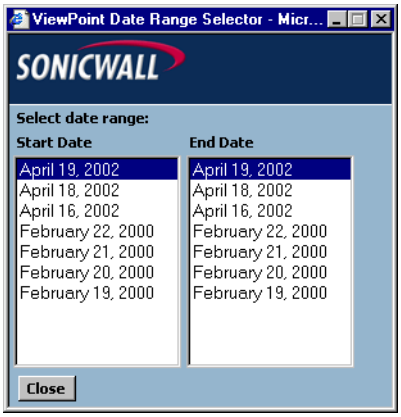
1. Start and log into ViewPoint.
2. Click the **Reports** tab.
3. Select the global icon, a group, or a SonicWALL appliance.
4. Expand the Attacks tree and click **Sources Over Time**. The Categories Over Time page appears (Figure 86).

Figure 88: Catagories Over Time Page



5. The bar graph displays the number of attacks attempted each day of the specified time period.
6. The table contains the following information:
   - **Source**—source of the attack.
   - **Attacks**—number of attacks.
   - **% of Attacks**—percentage of attacks from this source, compared to other sources. For example, if 2,000 attacks occurred during the time period and 1,000 attacks occurred from a source, its **% of Attacks** field will display 50%.
7. To change the date range of the report, click **Settings**. The Reporting Date Range Selector dialog box appears (Figure 87).

Figure 89: Report Settings Dialog Box



8. Select the starting and ending dates that you would like to view.
9. When you are finished, click **Close.** The GMS Reporting Module displays the report for the selected date range.

   Note: *These settings will stay in effect for all reports during your active login session.*

Viewing Authentication Reports

The login reports show user logins, administrator logins, and failed login attempts for users and administrators.

Note: *All reports appear in Universal Time, Coordinated (UTC) or Greenwich Mean Time (GMT).*

Select from the following:

- To view user logins, see “Viewing the User Login Report” on page 82.
- To view administrator logins, see “Viewing the Administrator Login Report” on page 83.
- To view failed login attempts, see “Viewing the Failed Login Report” on page 84.

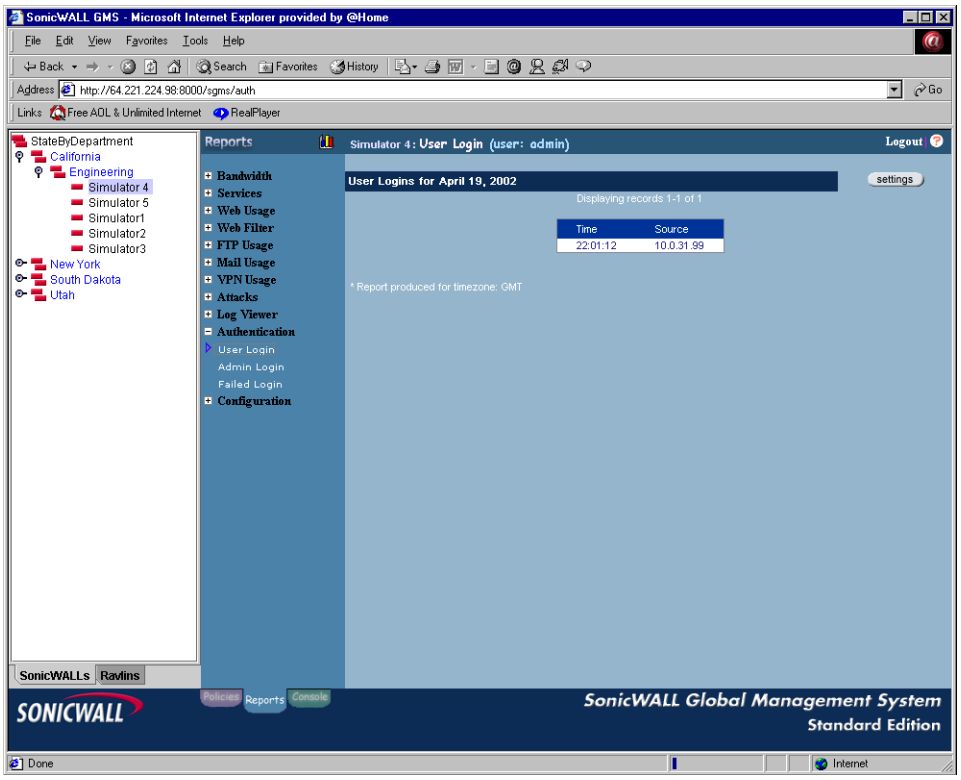
Viewing the User Login Report

The user login report shows users that logged on to the SonicWALL appliance during the specified day to bypass content filtering or to remotely access local network resources.

To view the User Login report, follow these steps:

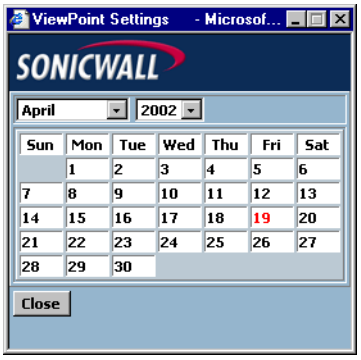
1. Start and log into ViewPoint.
2. Click the **Reports** tab.
3. Select a SonicWALL appliance.
4. Expand the Authentication tree and click **User Login**. The User Login page appears (Figure 90).

Figure 90: User Login Page



5. The table contains the following information:
   - **User**—the user name.
   - **Time**—time the user logged in.
6. The GMS Reporting Module shows today’s report. To change the date of the report, click **Settings**. The Report Settings dialog box appears (Figure 91).

Figure 91: Report Settings Dialog Box


ViewPoint Settings - Microsof...
SONICWALL
April
2002
Sun Mon Tue Wed Thu Fri Sat
1 2 3 4 5 6
7 8 9 10 11 12 13
14 15 16 17 18 19 20
21 22 23 24 25 26 27
28 29 30
Close

7. Select the year, month, and day that you would like to view.
8. When you are finished, click **Close.** The GMS Reporting Module displays the report for the selected day.

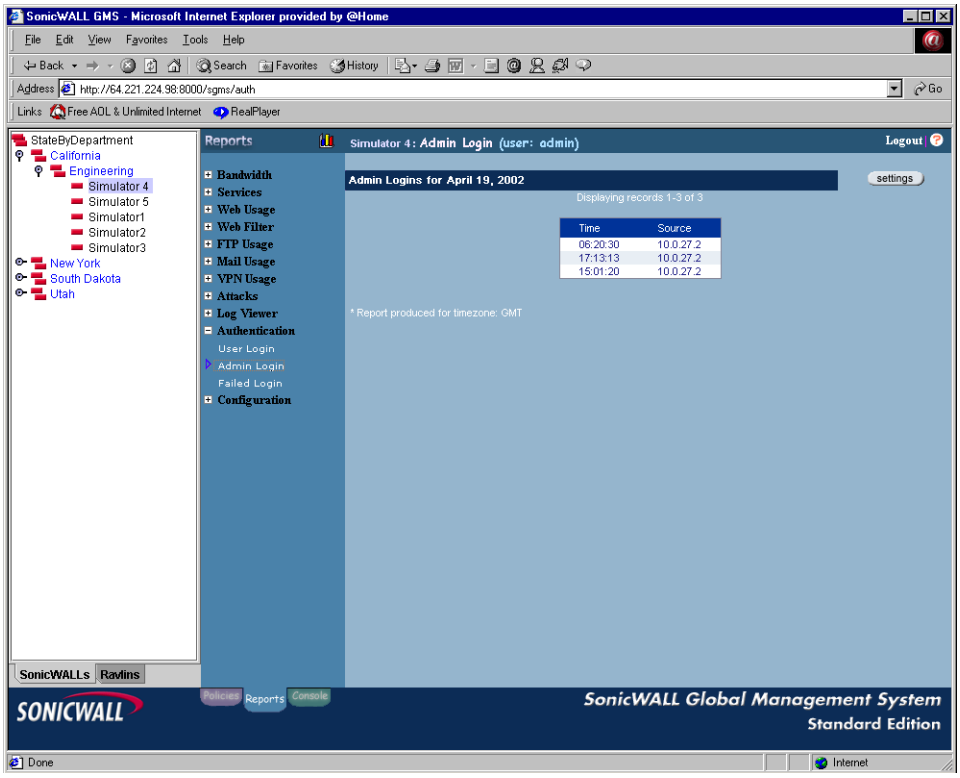
Viewing the Administrator Login Report

The administrator login report shows successful administrator logins during the specified day. This report is useful for identifying misuse and unauthorized management of a SonicWALL appliance.

To view the Admin Login report, follow these steps:

1. Start and log into ViewPoint.
2. Click the **Reports** tab.
3. Select a SonicWALL appliance.
4. Expand the Authentication tree and click **Admin Login**. The Admin Login page appears (Figure 92).

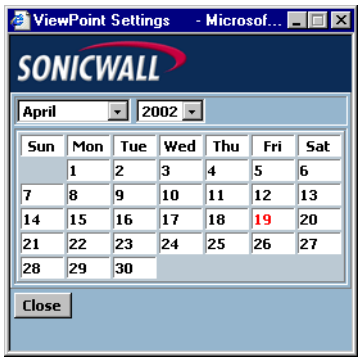
Figure 92: Admin Login Page



5. The table contains the following information:
   - **User**—the user name.
   - **Time**—time the user logged in.

6. The GMS Reporting Module shows today's report. To change the date of the report, click **Settings**. The Report Settings dialog box appears (Figure 93).

Figure 93: Report Settings Dialog Box


ViewPoint Settings - Microsof...
SONICWALL
April
2002
Sun Mon Tue Wed Thu Fri Sat
1 2 3 4 5 6
7 8 9 10 11 12 13
14 15 16 17 18 19 20
21 22 23 24 25 26 27
28 29 30
Close

7. Select the year, month, and day that you would like to view.
8. When you are finished, click **Close.** The GMS Reporting Module displays the report for the selected day.

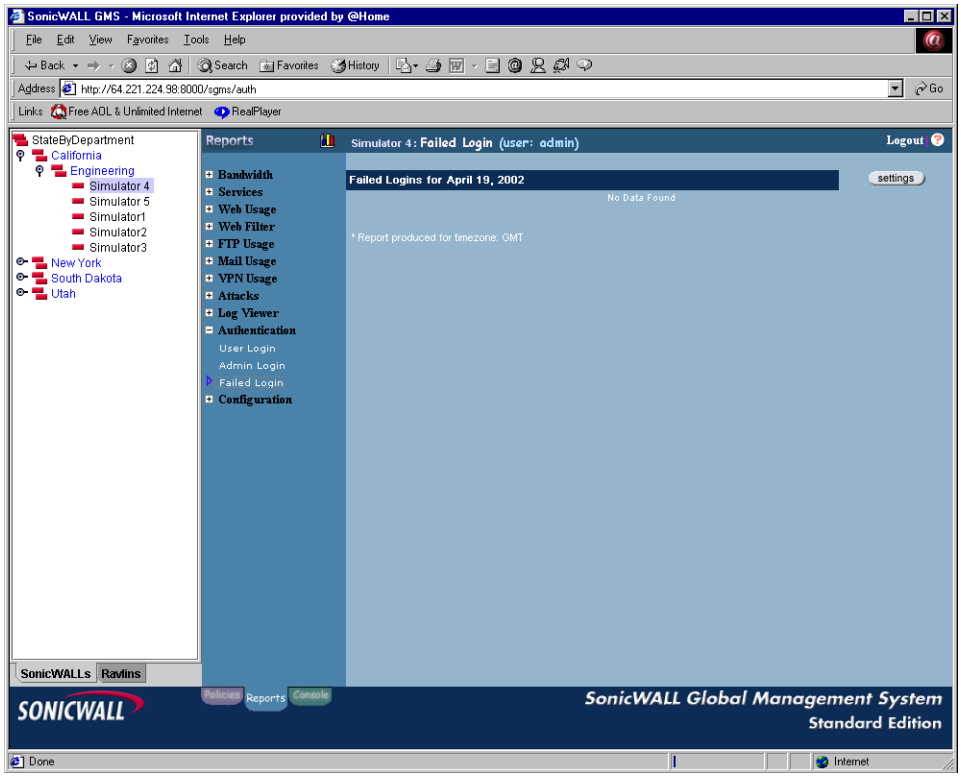
Viewing the Failed Login Report

The failed login reports shows failed login attempts for users and administrators that attempted to log on to the SonicWALL appliance during the specified day. This report is useful for identifying unauthorized access attempts and potentially malicious activity.

To view the Failed Login report, follow these steps:

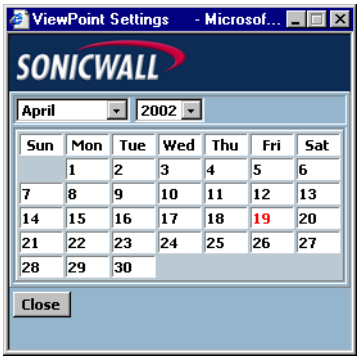
1. Start and log into ViewPoint.
2. Click the **Reports** tab.
3. Select a SonicWALL appliance.
4. Expand the Authentication tree and click **Failed Login**. The Failed Login page appears (Figure 94).

Figure 94: Failed Login Page



5. The table contains the following information:
   - **User**—the user name.
   - **Time**—time the user logged in.
   - **IP Address**—IP address of the user.
6. The GMS Reporting Module shows today's report. To change the date of the report, click **Settings**. The Report Settings dialog box appears (Figure 95).

   Figure 95: Report Settings Dialog Box


ViewPoint Settings - Microsof...
SONICWALL
April
2002
Sun Mon Tue Wed Thu Fri Sat
1 2 3 4 5 6
7 8 9 10 11 12 13
14 15 16 17 18 19 20
21 22 23 24 25 26 27
28 29 30
Close

7. Select the year, month, and day that you would like to view.
8. When you are finished, click **Close.** The GMS Reporting Module displays the report for the selected day.

Viewing the Log

The Log Viewer contains detailed information on each transaction that occurred on the SonicWALL appliance or Ravlin device. This information is stored for the time that you specified in the configuration settings.

Note: *The Log Viewer displays raw log information for every connection. Depending on the amount of traffic, this can quickly consume a large amount of space in the database. It is highly recommended to be careful when choosing the number of days of information that will be stored. For more information, see "Configuring GMS Reporting Module Settings" on page 12.*

Select from the following:

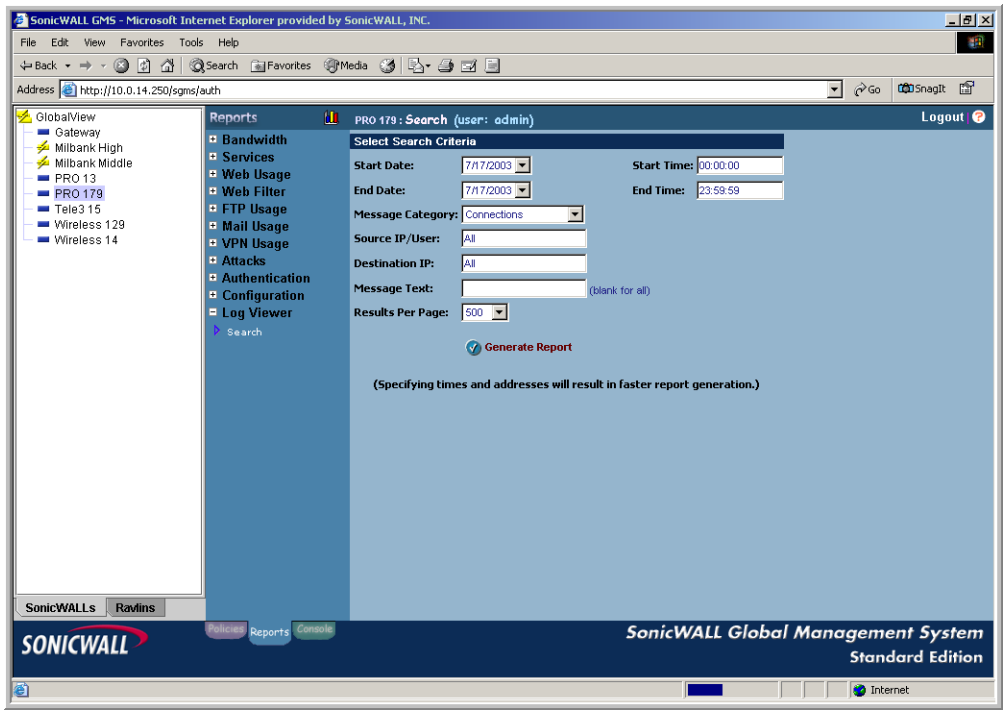
- To view the log for a SonicWALL appliance, see "Viewing the Log for a SonicWALL Appliance" on page 86.
- To view the log for a Ravlin device, see "Viewing the Log for a Ravlin Device" on page 87.

Viewing the Log for a SonicWALL Appliance

To view the Log, follow these steps:

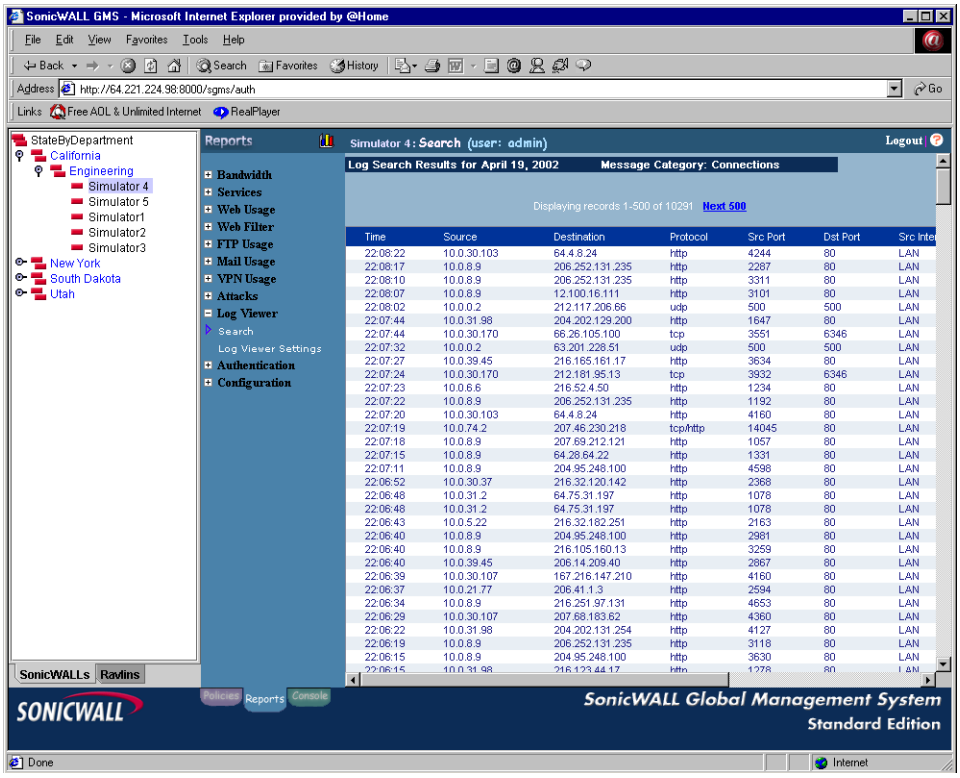
1. Start and log into ViewPoint.
2. Click the **Reports** tab.
3. Select a SonicWALL appliance.
4. Expand the Log Viewer tree and click **Search**. The Search page appears (Figure 96).

Figure 96: Search Page



5. Select the date to view from the **Date** list box.
6. Enter the starting time of events to view in the **Start Time** field.
7. Enter the ending time of events to view in the **End Time** field.
8. Select the type of events to view from the **Message Category** list box.
9. Enter the source IP address to view in the **Source IP Address** field. To view all IP addresses, enter All.
10. Enter the destination IP address to view in the **Destination IP Address** field. To view all IP addresses, enter All.
11. Select the number of entries to display per page from the **Results Per Page** field.
12. Click **Generate Report**. The Log Viewer Results page appears (Figure 97).

Figure 97: Log Viewer Results Page



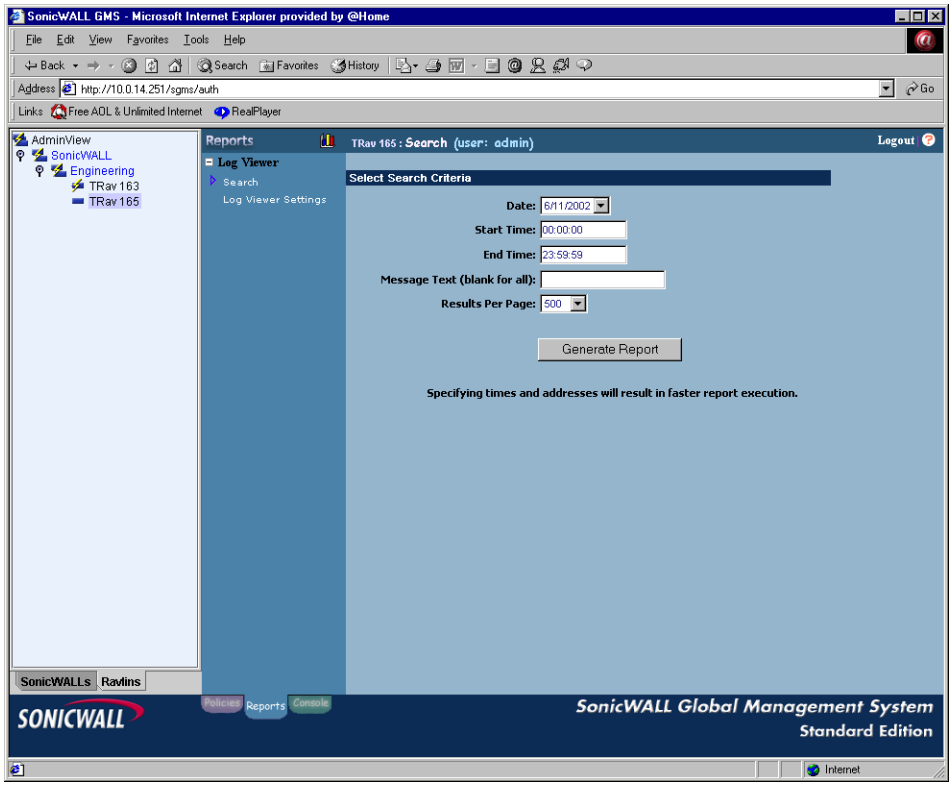
13. Search through the entries to find the information for which you are searching. To view the next page of entries, click **Next**.
14. To generate another report, click **Search** again in the Log Viewer Tree.

Viewing the Log for a Ravlin Device

To view the Log, follow these steps:

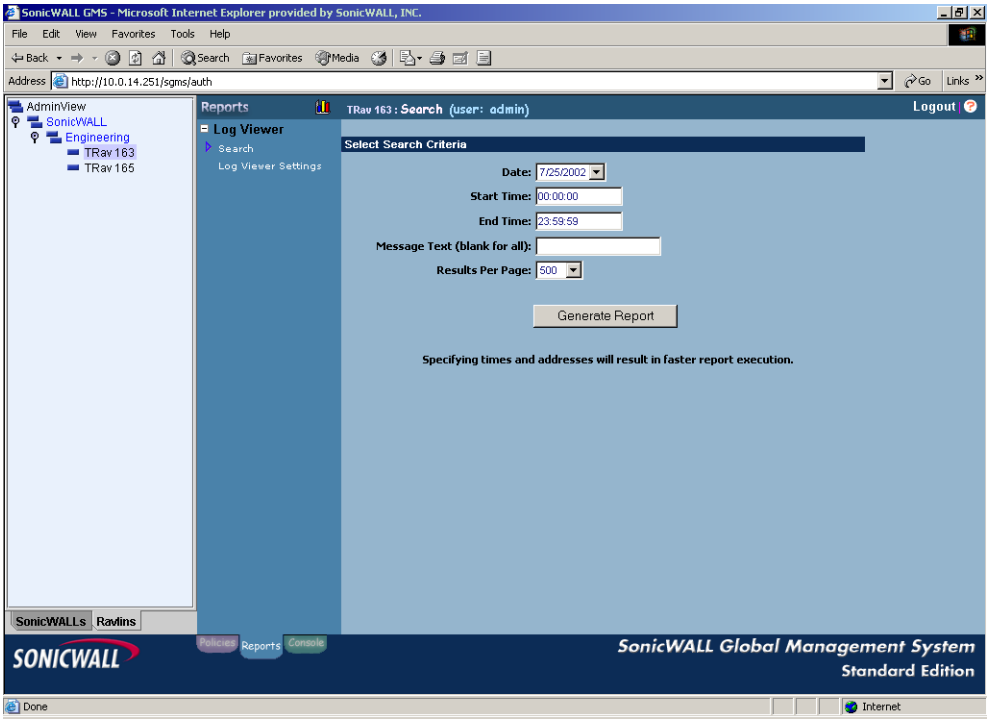
1. Start and log into ViewPoint.
2. Click the **Reports** tab.
3. Select a Ravlin device.
4. Expand the Log Viewer tree and click **Search**. The Search page appears (Figure 98).

Figure 98: Search Page



5. Select the date to view from the **Date** list box.
6. Enter the starting time of events to view in the **Start Time** field.
7. Enter the ending time of events to view in the **End Time** field.
8. Select the type of events to view from the **Message Category** list box.
9. Enter the source IP address to view in the **Source IP Address** field. To view all IP addresses, enter All.
10. Enter the destination IP address to view in the **Destination IP Address** field. To view all IP addresses, enter All.
11. Select the number of entries to display per page from the **Results Per Page** field.
12. Click **Generate Report**. The Log Viewer Results page appears (Figure 97).

Figure 99: Log Viewer Results Page



13. Search through the entries to find the information for which you are searching. To view the next page of entries, click **Next**.
14. To generate another report, click **Search** again in the Log Viewer Tree.

Note: *See Appendix A for the list of available message texts.*

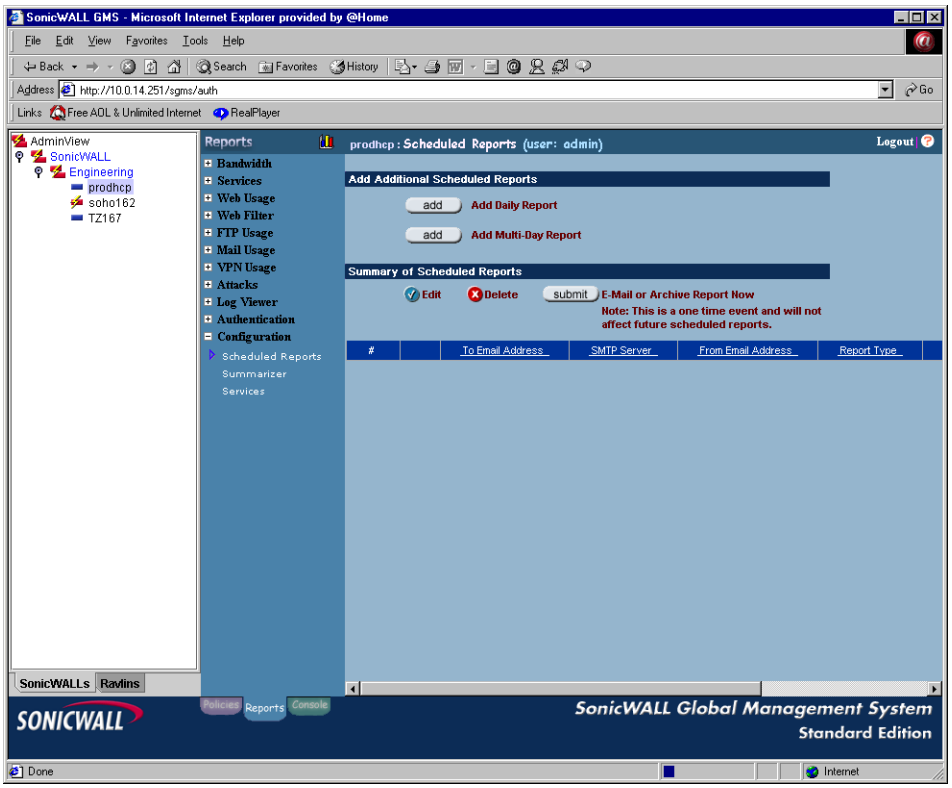
Scheduling GMS Reporting

Standalone ViewPoint (ViewPoint) Reporting can automatically send reports to any e-mail addresses that you specify.

To view currently scheduled reports or configure new reports, follow these steps:

1. Start and log into ViewPoint.
2. Click the **Reports** tab.
3. Select a SonicWALL appliance.
4. Expand the Configuration tree and click **Scheduled Reports**. The Scheduled Reports page appears (Figure 100).

Figure 100: Scheduled Reports Page



5. The Scheduled Reports page contains a list of currently scheduled reports. To edit a report, select its radio button and click **Edit**. To delete a report, select its radio button and click **Delete**.

   Note: *Scheduled reports are identified by their email addresses. Therefore, modifying the email address for a scheduled report creates another scheduled report.*

6. To e-mail a currently scheduled report now, click **E-mail Reports Now**.

   Note: *This will not affect the normally scheduled report.*

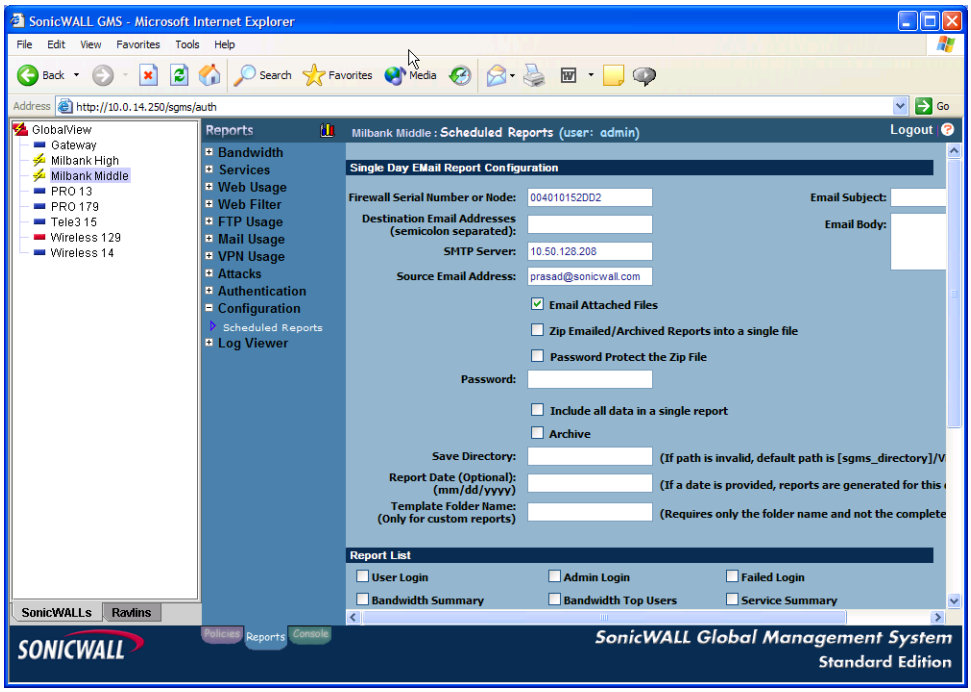
7. Select from the following:
   - To create a new daily report, see “Scheduling a Daily Report” on page 92.
   - To create a new weekly or monthly report, see “Scheduling a Weekly or Monthly Report” on page 93.

Scheduling a Daily Report

Daily reports are sent out once a day at 03:00 GMT and contain information for the previous day. To configure a new daily report, follow these steps:

1. From the Scheduled Reports page, click the **Add Daily Report** button. The Daily Reports page appears (Figure 101).

   Figure 101: Daily Reports Page



2. Enter the Destination e-mail addresses in the **Destination Email Addresses** field. Make sure each e-mail address is separated by a semicolon (;).
3. By default, the GMS Reporting Module will use the Simple Mail Transfer Protocol (SMTP) server that was specified during ViewPoint installation. To change it, enter the IP address or hostname of the SMTP server in the **SMTP Server Address** field.
4. By default, the GMS Reporting Module will use the e-mail address of the user logged into ViewPoint as the Sender e-mail address. To change it, enter a new Sender e-mail address in the **Source Email Address** field.
5. Enter the Subject Line that will appear in reports sent from the GMS Reporting Module in the **Email Subject** field.
6. Enter text that will appear in the message body in the **Email Body** field.
7. To send the file as an email attachment, select the **Email Attached File** check box.
8. To compress the reports into a single file, select the **Zip Emailed/Archived Reports into a single file** check box.

   To password-protect the Zip file, select the **Password Protect the Zip File** check box and enter the password in the **Password** field.

   To include all of the data in a single report, select the **Include all data in a single report** check box.
9. To archive the file on the server’s hard disk, select the **Archive** check box and enter a path in the **Save Directory** field.

   Specify the directory where the file will be archive in the **Save Directory** field.
10. **Optional.** To specify a specific date, enter the date in the **Report Date** field.

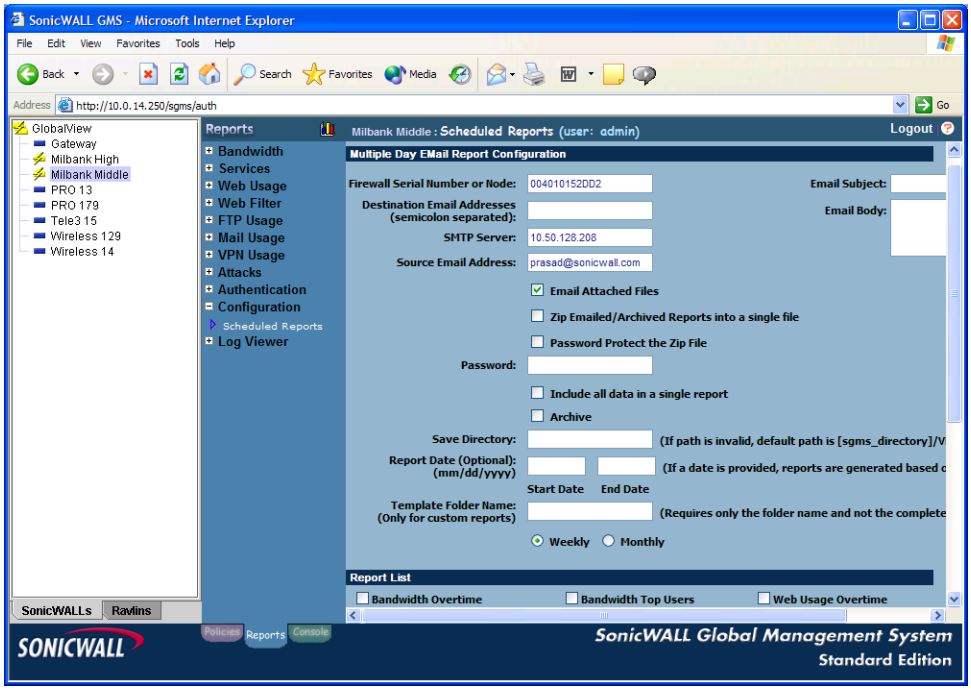
11. If you are using custom reports, specify the folder location of the template files in the **Template Folder Name** field. For more information, see Chapter 5, "Scheduling GMS Reporting."
12. Select the daily reports that will be included in the e-mail message:
    - **User Login**—shows users that logged on to the SonicWALL appliance to bypass content filtering or to remotely access local network resources.
    - **Admin Login**—shows successful administrator logins for the SonicWALL appliance.
    - **Failed Login**—shows failed login attempts for users and administrators that attempted to log on through the SonicWALL appliance.
    - **Bandwidth Summary**—amount of traffic handled by the SonicWALL appliance during each hour.
    - **Bandwidth Top Users**—displays the users who used the most bandwidth.
    - **Service Summary**—amount of traffic handled by each service during each hour.
    - **Web Usage Summary**—amount of HTTP bandwidth handled by the SonicWALL appliance during each hour of the day.
    - **Web Usage Top Sites**—displays the web sites that used the most HTTP bandwidth.
    - **Web Usage Top Users**—displays the users who used the most HTTP bandwidth.
    - **Web Usage Sites By User**—displays a list of all users, their top sites, the number of hits to each site, and the amount of data transferred.
    - **Web Filter Summary**—displays the number of times users attempt to access blocked sites during each hour.
    - **Web Filter Top Sites**—displays the top blocked web sites that users attempted to access.
    - **Web Filter Top Users**—displays the users who made the most attempts to access blocked sites.
    - **Web Filter Sites By User**—displays a list of all users, their top sites, and the number of attempts that were made to access each site.
    - **FTP Usage Summary**—amount of FTP bandwidth handled by the SonicWALL appliance.
    - **FTP Usage Top Users**—displays the users who used the most FTP bandwidth.
    - **Mail Usage Summary**—amount of mail handled by the SonicWALL appliance.
    - **Mail Usage Top Users**—displays the users who sent and received the most mail.
    - **Attacks Summary**—number of attack attempted on the SonicWALL appliance.
    - **Attacks By Category**—displays the attacks that occurred, sorted by category.
    - **Attacks By Source**—displays the top sources of attacks.
    - **Attacks Dropped Packets**—number of dropped packets on the SonicWALL appliance.
13. When you are finished, click **Add**. The new report will appear in the list on the Scheduled Reports page.

Scheduling a Weekly or Monthly Report

Weekly reports are sent out every Sunday at 03:00 GMT and contain information for the previous week. Monthly reports are sent out on the first day of every month at 03:00 GMT and contain information for the previous month. To configure a new weekly or monthly report, follow these steps:

1. From the Scheduled Reports page, click the **Add Multi-Day Report** button. The Multi-Day Reports page appears (Figure 102).

Figure 102: Multi-Day Reports Page



2. Enter the Destination e-mail addresses in the **Destination Email Addresses** field. Separate each e-mail address with a semicolon (;).
3. Enter the IP address or hostname of the Simple Mail Transfer Protocol (SMTP) server in the **SMTP Server Address** field.
4. Enter the Sender e-mail address that will appear in messages sent from the GMS Reporting Module in the **Source Email Address** field.
5. Enter the Subject Line that will appear in reports sent from the GMS Reporting Module in the **Email Subject** field.
6. Enter text that will appear in the message body in the **Email Body** field.
7. To send the file as an email attachment, select the **Email Attached File** check box.
8. To compress reports into a single file, select the **Zip Emailed/Archived Reports into a single file** check box.

   To password-protect the Zip file, select the **Password Protect the Zip File** check box and enter the password in the **Password** field.

   To include all of the data in a single report, select the **Include all data in a single report** check box.
9. To archive the file to hard disk, select the **Archive** check box and enter a path in the **Save Directory** field.

   Specify the directory where the file will be archive in the **Save Directory** field.
10. **Optional.** To specify a specific date, enter the date in the **Report Date** field.
11. If you are using custom reports, specify the folder location of the template files in the **Template Folder Name** field. For more information, see Chapter 5, “Scheduling GMS Reporting.”
12. Select whether the report will be sent **Weekly** or **Monthly**.
13. Select the reports that will be included in the e-mail message:
    - **Bandwidth Overtime**—displays the daily amount of traffic handled by the SonicWALL appliance for the week or month.
    - **Web Usage Overtime**—displays the daily amount of HTTP bandwidth handled by the SonicWALL appliance for the week or month.
    - **Web Filter Overtime**—displays the number of attempts that were made to access blocked web sites for the week or month.
    - **FTP Usage Overtime**—displays the daily amount of FTP bandwidth handled by the SonicWALL appliance for the week or month.

- **Mail Usage Overtime**—displays the daily amount of mail handled by the SonicWALL appliance for the week or month.
- **Attacks Overtime**—displays the daily number of attacks attempted during the week or month.
- **Drop Packets Overtime**—displays the number of packet errors during the week or month.
- **VPN Overtime**—displays daily number of VPN connections during the week or month.

14. When you are finished, click **Add**. The new report will appear in the list on the Scheduled Reports page.

Customizing Report Elements

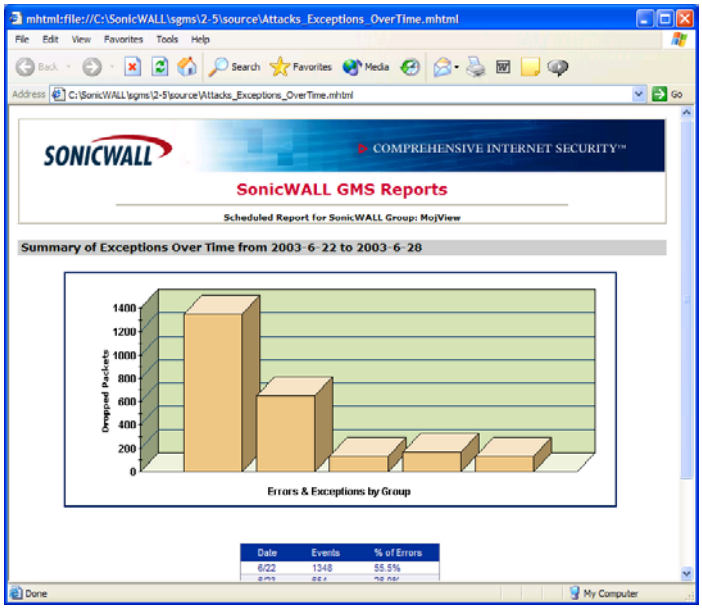
The GMS Reporting Module contains many elements that can be customized to meet the look and feel of your organization's corporate image. The elements that can be customized include:

Table 1: Custom Elements

Element	Default	Description
[PAGE_BG_COLOR]	#FFFFFF	Page background color
[HEADING]	SonicWALL GMS Reports	Heading Color and Title
[LOGO]	images/mainLogo2.gif	Main logo at top of page.
[LOGO_DESCRIPTION]	SonicWALL GMS Reports	Logo description.
[LOGO_HREF]	http://www.sonicwall.com	The location to which the user is taken when he or she clicks the logo.
[LOGO_TABLE_BG_COLOR]	#FFFFFF	Background color of the table in which the logo resides.
[TITLE_BAR_BG_COLOR]	#CCCCCC	Color of the title bar.
[TITLE_BAR_FONT_COLOR]	#000000	Color of the font in the title bar.
[TITLE_BAR_FONT_SIZE]	2	Size of the Font in the title bar.
[CHART_BG_COLOR]	#FFFFFF	Background color of the chart.
[CHART_PLOT_COLOR]	#D7E1B2	Color of the bar in the bar graphs.
[PIE_PLOT_COLOR]	#FFFFFF	Color of the pie in pie graphs.
[TABLE_HEADING_COLOR]	#003399	Color of the table heading.
[TABLE_EVEN_ROW_COLOR]	#FFFFFF	Color of the even-numbered rows.
[TABLE_ODD_ROW_COLOR]	#E8EEF4	Color of the odd-numbered rows.
[TABLE_TOTAL_ROW_COLOR]	#003399	Color of the "total" row.
[FOOTER_FONT_COLOR]	#000000	Color of the footer font.
[FOOTER_FONT_SIZE]	1	Size of the footer font.

The following figure shows the report elements as they are displayed.

Figure 103: Report Elements



Using the Reporting Customization Tool

This section describes how to use the Reporting Customization Tool. You can use the tool to create multiple templates. After creating a template, you can apply it to one, some, or all reports.

To use the Reporting Customization Tool, follow these steps:

1. Create a folder to store custom report templates. The folder name cannot contain spaces and must be located in the appropriate directory. For example, to use the folder name MyCustomReports, you must create the folder with the following directory structure:
   `<gms_directory>\Tomcat\webapps\sgms\reports\scheduledreports\MyCustomReports`
2. Create a text file that contains all the attributes and values that can be customized. For more information, see the params.txt file that accompanied the Reporting Customization Tool.
3. Enter the following command:
   `ReportTool.bat input_file target_folder`

   where *input_file* is the name of the text file that you customized and *target_folder* is the name of the target folder.

   Note: Do not specify the complete path to the folder.
4. The default logo used in the reports is the SonicWALL logo. If you wish to use a different logo and other graphics, copy them into the following directory: **`\sgms\images\`**.
5. Restart the SGMS Web server service.
6. Set the template folder name in the report schedule created to this folder name. This must be set for all the report schedules that use the customized templates.

Scheduling a Report

For information on scheduling a custom report, see Chapter 4, “Scheduling GMS Reporting.”

Technical Tips

Forwarding Syslog Data to Another Syslog Server

To forward ViewPoint syslog data to another syslog server, follow these steps:

1. Open the sgmsConfig.xml file with a text editor.
2. Locate the following line:

   ```
   Parameter name =“syslog.forwardToHost” value=“”
   ```

3. Add the IP address or hostname of the destination syslog server to the value attribute.
4. Save the sgmsConfig.xml file and exit.
5. Ensure that at least firmware 6.3.1.0 is running on the managed SonicWALL appliances.

Note: *To configure ViewPoint to not store the syslog data after it has been forwarded, you must disable he GMS Reporting Module. To do this, open the* ***SGMS Settings*** *page in the Console Panel, deselect the* ***Enable Reporting*** *check box, and click* ***Update****.*

Forwarding the Syslog Date to a WebTrends Server

From ViewPoint, you can forward the syslog data to a WebTrends server. To acomplish this, do the following:

1. Open the sgmsConfig.xml file with a text editor.
2. Locate the following line:

   ```
   Parameter name =“syslog.forwardToHost” value=“”
   ```

3. Add the IP address or hostname of the WebTrends syslog to the value attribute.
4. Save the sgmsConfig.xml file and exit.
5. Ensure that at least firmware 6.3.1.0 is running on the managed SonicWALL appliances.
6. Change the syslog format in each managed SonicWALL appliance from the default format to the WebTrends format on the Log Settings page.

   WebTrends cannot read the SonicWALL syslog in its default format. The default syslog format’s source (src) and destination (dst) fields contain port numbers and link information (i.e., WAN, LAN, and DMZ). These prevent WebTrends from resolving the IP to DNS entries and from performing HTML title lookups within the reports.

Note: *The GMS Reporting Module also has problems with the WebTrends syslog format. To disable GMS Reporting, open the* ***SGMS Settings*** *page in the Console Panel, deselect the* ***Enable Reporting*** *check box, and click* ***Update****.*

Posting GMS Reporting to Another Web Server for End-User Access

To allow end user access to another web server for end-user access, install the ViewPoint Console in redundant mode.

You can then allow end user access to the redunant Console for viewing GMS Reporting real-time and historical reports. End user access will be isolated from the main Console that is used for managing and configuring SonicWALL appliances.

Syslog Messages for

Firmware 6.5

SonicWALL activated

Log Cleared

Log successfully sent via email

Log full; deactivating SonicWALL

New URL List loaded

No new URL List available

Problem loading the URL List; check Filter settings

Problem loading the URL List; check your DNS server

Problem sending log email; check log settings

Restarting SonicWALL; dumping log to email

Web site blocked

Newsgroup blocked

Web site accessed

Newsgroup accessed

ActiveX blocked

Java blocked

ActiveX or Java archive blocked

Cookie removed

Ping of death blocked

IP spoof detected

Illegal LAN address in use

Possible SYN flood attack

Probable SYN flood attack

Land Attack Dropped

Fragmented Packet Dropped

Successful administrator login

Administrator login failed - incorrect password

Successful local user login

User login failed - incorrect password

Unknown user attempted to log in

Login screen timed out

Attempted administrator login from %s

TCP connection dropped

UDP packet dropped

ICMP packet dropped

PPTP packet dropped
IPSec packet dropped
Unknown protocol dropped
IPSec packet dropped; waiting for pending IPSec connection
IPSec connection interrupt
NAT could not remap incoming packet
ARP timeout
Broadcast packet dropped
No ICMP redirect sent
Out-of-order command packet dropped
Failure to add data channel
RealAudio decode failure
Duplicate packet dropped
No HOST tag found in HTTP request
The cache is full; %d open connections; some will be dropped
Code:
Type:
Source:
Destination:
License exceeded: Connection dropped because too many IP addresses are in use on your LAN
Rule
Access to Proxy Server Blocked
Diagnostic Code E
Dynamic IPSec client connected
Received fragmented packet or fragmentation needed
Diagnostic Code D
Illegal IPSec SPI
Unknown IPSec SPI
IPSec Authentication Failed
IPSec Decryption Failed
Incompatible IPSec Security Association
IPSec packet from or to an illegal host
SPI:
NetBus Attack Dropped
Back Orifice Attack Dropped
Net Spy Attack Dropped
Sub Seven Attack Dropped
Ripper Attack Dropped
Striker Attack Dropped
Senna Spy Attack Dropped
Priority Attack Dropped
Ini Killer Attack Dropped
Smurf Amplification Attack Dropped
Possible Port Scan Dropped
Probable Port Scan Dropped
Failed to resolve name
local range:
remote range:

IKE Responder: Accepting IPSec proposal (Phase 2)
IKE Responder: IPSec proposal does not match (Phase 2)
IKE negotiation complete. Adding IPSec SA. (Phase 2)
Starting IKE negotiation
Deleting IPSec SA for destination
Deleting IPSec SA
Diagnostic Code A
Diagnostic Code B
Diagnostic Code C
Status
#Web site hit
Connection Opened
Retransmitting DHCP DISCOVER.
Retransmitting DHCP REQUEST (Requesting).
Retransmitting DHCP REQUEST (Renewing).
Retransmitting DHCP REQUEST (Rebinding).
Retransmitting DHCP REQUEST (Rebooting).
Retransmitting DHCP REQUEST (Verifying).
Sending DHCP DISCOVER.
DHCP Server not available. Did not get any DHCP OFFER.
Got DHCP OFFER. Selecting.
Sending DHCP REQUEST.
DHCP Client did not get DHCP ACK.
DHCP Client got NACK.
DHCP Client got ACK from server.
DHCP Client is declining address offered by the server.
DHCP Client sending REQUEST and going to REBIND state.
DHCP Client sending REQUEST and going to RENEW state.
Sending DHCP REQUEST (Renewing).
Sending DHCP REQUEST (Rebinding).
Sending DHCP REQUEST (Rebooting).
Sending DHCP REQUEST (Verifying).
DHCP Client failed to verify and lease has expired. Go to INIT state.
DHCP Client failed to verify and lease is still valid. Go to BOUND state.
DHCP Client got a new IP address lease.
Sending DHCP RELEASE.
Access attempt from host without Anti-Virus agent installed
Anti-Virus agent out-of-date on host
Received AV Alert: %s
Unused AV log entry.
Starting PPPoE discovery
PPPoE LCP Link Up
PPPoE LCP Link Down
PPPoE terminated
PPPoE Network Connected
PPPoE Network Disconnected
PPPoE discovery process complete
PPPoE starting CHAP Authentication

PPPoE starting PAP Authentication
PPPoE CHAP Authentication Failed
PPPoE PAP Authentication Failed
Wan IP Changed
XAUTH Succeeded with VPN client
XAUTH Failed with VPN client, Authentication failure
XAUTH Failed with VPN client, Cannot Contact RADIUS Server
Log Debug
Add an attack message
Primary firewall has transitioned to Active
Backup firewall has transitioned to Active
Primary firewall has transitioned to Idle
Backup firewall has transitioned to Idle
Primary missed heartbeats from Active Backup: Primary going Active
Backup missed heartbeats from Active Primary: Backup going Active
Primary received error signal from Active Backup: Primary going Active
Backup received error signal from Active Primary: Backup going Active
Backup firewall being preempted by Primary
Primary firewall preempting Backup
Active Backup detects Active Primary: Backup going Idle
Imported HA hardware ID did not match this firewall
Discovered HA Backup Firewall
HA Peer Firewall Synchronized
Error Synchronizing HA Peer Firewall
Received AV Alert: Your SonicWALL Network Anti-Virus subscription has expired. %s
Primary received heartbeat from wrong source
Backup received heartbeat from wrong source
HA packet processing error
Heartbeat received from incompatible source
Diagnostic Code F
Forbidden E-Mail attachment disabled
PPPoE PAP Authentication success.
PPPoE PAP Authentication Failed. Please verify PPPoE username and password
Disconnecting PPPoE due to traffic timeout
No response from ISP Disconnecting PPPoE.
Backup going Active in preempt mode after reboot
VPN Log
VPN Log Debug
Denied TCP connection from LAN
Denied UDP packet from LAN
Denied ICMP packet from LAN
Firewall access from LAN
Probable TCP FIN scan
Probable TCP XMAS scan
Probable TCP NULL scan
IPSEC Replay Detected
TCP FIN packet dropped
Received a path MTU icmp message from router/gateway

Problem loading the URL List; Appliance not registered.
Problem loading the URL List; Subscription expired.
Problem loading the URL List; Try loading it again.
Problem loading the URL List; Retrying later.
Problem loading the URL List; Flash write failure.
Received a path MTU icmp message from router/gateway
MTU:
The loaded content URL List has expired.
Error setting the IP address of the backup, please manually set to backup LAN IP
Error updating HA peer configuration
Fraudulent Microsoft Certificate Blocked
VPN TCP SYN
VPN TCP FIN
VPN TCP PSH
Content filter subscription expired.
New firmware available.
Successful administrator login from the CLI
Administrator login failed - incorrect password from the CLI
L2TP Tunnel Negotiation Started
L2TP Session Negotiation Started
L2TP Max Retransmission Exceeded
L2TP Tunnel Established
L2TP Tunnel Disconnect from Remote
L2TP Session Established
L2TP Session Disconnect from Remote
L2TP PPP Negotiation Started
L2TP LCP Down
L2TP PPP Session Up
L2TP PPP Down
L2TP PPP Authentication Failed
L2TP LCP Up
L2TP Disconnect Initiated by the User
Disconnecting L2TP Tunnel due to traffic timeout
L2TP Connect Initiated by the User
L2TP PPP link down
Primary WAN link down, Primary going Idle
Backup WAN link down, Primary going Active
Primary WAN link down, Backup going Active
Primary WAN link up, preempting Backup
DHCP RELEASE relayed to Central Gateway
DHCP lease relayed to local device
DHCP RELEASE received from remote device
DHCP lease relayed to remote device
DHCP lease to LAN device conflicts with remote device, deleting remote IP entry
WARNING: DHCP lease relayed from Central Gateway conflicts with IP in Static Devices list
DHCP lease dropped. Lease from Central Gateway conflicts with Relay IP
IP spoof detected on packet to Central Gateway, packet dropped
Request for Relay IP Table from Central Gateway

Requesting Relay IP Table from Remote Gateway
Sent Relay IP Table to Central Gateway
Obtained Relay IP Table from Remote Gateway
Failed to synchronize Relay IP Table
Successful administrator login
Successful administrator login
Successful remote user login
Successful remote user login
NAT Discovery : Peer IPSec Security Gateway behind a NAT/NAPT Device
NAT Discovery : Local IPSec Security Gateway behind a NAT/NAPT Device
NAT Discovery : No NAT/NAPT device detected between IPSec Security gateways
NAT Discovery : Peer IPSec Security Gateway doesn't support VPN NAT Traversal
User login failed - RADIUS authentication failure
User login failed - RADIUS server timeout
User login failed - RADIUS configuration error
User login failed - User has no privileges for login from that location
IPSec packet from an illegal host
Forbidden E-Mail attachment deleted
IKE Responder: Mode %d - not tunnel mode
IKE Responder: No matching Phase 1 ID found for proposed remote network
IKE Responder: Proposed remote network is 0.0.0.0 but not DHCP relay nor default route
IKE Responder: No match for proposed remote network address
IKE Responder: Default LAN gateway is set but peer is not proposing to use this SA as a default route
IKE Responder: Tunnel terminates outside firewall but proposed local network is not NAT public address
IKE Responder: Tunnel terminates inside firewall but proposed local network is not inside firewall
IKE Responder: Tunnel terminates on DMZ but proposed local network is on LAN
IKE Responder: Tunnel terminates on LAN but proposed local network is on DMZ
IKE Responder: AH Perfect Forward Secrecy mismatch
IKE Responder: ESP Perfect Forward Secrecy mismatch
IKE Responder: Algorithms and/or keys do not match
Administrator logged out
Administrator logged out - inactivity timer expired
User logged out
User logged out - max session time exceeded
User logged out - inactivity timer expired
NAT device may not support IPSec AH passthrough
TCP Xmas Tree Blocked
CFL auto-download disabled, time problem detected
Requesting CRL from
CRL Loaded from
Failed to get CRL from
Not enough memory to hold the CRL
Connection timed out
Cant connect to the CRL server
Unknown reason
Failed to Process CRL from
Bad CRL format
Issuer match failed

Certificate on Revoked list(CRL)

No Certificate for

PPP Dial-Up: Dialing: %s

PPP Dial-Up: No dialtone detected - check phone-line connection

PPP Dial-Up: No link carrier detected - check phone number

PPP Dial-Up: Dialed number is busy

PPP Dial-Up: Dialed number did not answer

PPP Dial-Up: Connected at %s bps - starting PPP

PPP Dial-Up: Unknown dialing failure

PPP Dial-Up: Link carrier lost

PPP: Authentication successful

PPP: PAP Authentication failed - check username / password

PPP: CHAP authentication failed - check username / password

PPP: MS-CHAP authentication failed - check username / password

PPP: Starting MS-CHAP authentication

PPP: Starting CHAP authentication

PPP: Starting PAP authentication

PPP Dial-Up: PPP negotiation failed - disconnecting

PPP Dial-Up: Idle time limit exceeded - disconnecting

PPP Dial-Up: Failed to get IP address

PPP Dial-Up: Received new IP address

PPP Dial-Up: PPP link established

PPP Dial-Up: PPP link down

PPP Dial-Up: Shutting down link

PPP Dial-Up: Initialization : %s

PPP Dial-Up: User requested disconnect

PPP Dial-Up: User requested connect

PPP Dial-Up: Connect request canceled

The network connection in use is %s

L2TP Server : L2TP Tunnel Established.

L2TP Server : L2TP Session Established.

L2TP Server : L2TP PPP Session Established.

L2TP Server: Radius reports Authentication Failure

L2TP Server: Local Authentication Failure

L2TP Server: Radius server not assigned IP address

L2TP Server: No IP address available in the Local IP Pool

L2TP Server: L2TP Tunnel Disconnect from the Remote.

L2TP Server: L2TP Session Disconnect from the Remote.

L2TP Server: L2TP Remote terminated the PPP session

L2TP Server: Local Authentication Success.

L2TP Server: Radius Authentication Success

L2TP Server: Keep alive Failure. Closing Tunnel

PPP Dial-Up: Manual intervention needed. Check Primary Profile or Profile details

PPP Dial-Up: Trying to failover but Primary Profile is manual

PPP Dial-Up: Startup without Ethernet cable, will try to dial on outbound traffic

PPP Dial-Up: Dial initiated by %s

The current WAN interface is not ready to route packets.

Probing failure on %s

PPP Dial-Up: Maximum connection time exceeded - disconnecting

Adminstrator name changed

User login failure rate exceeded - source address locked out

PPP Dial-Up: The profile in use disabled VPN networking.

PPP Dial-Up: VPN networking restored.

%s Ethernet Port Up

%s Ethernet Port Down

L2TP Server: Call Disconnect from Remote.

L2TP Server: Tunnel Disconnect from Remote.

L2TP Server : Deleting the Tunnel

L2TP Server : Deleting the L2TP active Session

L2TP Server : Retransmission Timeout, Deleting the Tunnel

NAT translated packet exceeds size limit, packet dropped

HTTP management port has changed

HTTPS management port has changed

IKE Responder: Mode %d - not transport mode. Xauth is required but not supported by peer.

L2TP Server : Access from L2TP VPN Client Privilege not enabled for Radius Users.

L2TP Server : User Name authentication Failure locally.

IKE Responder: Tunnel terminates outside firewall but proposed remote network is not NAT public address

IKE Initiator: Start Quick Mode (Phase 2).

Port configured to receive IPSEC ONLY. Drop packet received in the clear.

Imported VPN SA is invalid - disabled

IPSEC SA lifetime expired.

IKE SA lifetime expired.

IKE Initiator: Start Main Mode negotiation (Phase 1)

IKE Responder: Received Quick Mode Request (Phase 2)

IKE Initiator: Main Mode complete (Phase 1)

IKE Initiator: Aggressive Mode complete (Phase 1).

IKE Responder: Received Main Mode request (Phase 1)

IKE Responder: Received Aggressive Mode request (Phase 1)

IKE Responder: Main Mode complete (Phase 1)

IKE Initiator: Start Aggressive Mode negotiation (Phase 1)

Entering FIPS ERROR state

Crypto DES test failed

Crypto DH test failed

Crypto Hmac-MD5 fest failed

Crypto Hmac-Sha1 test failed

Crypto RSA test failed

Crypto Sha1 test failed

Crypto hardware DES test failed

Crypto Hardware 3Des test failed

Crypto Haredware DES with SHA test failed

Crypto Hardware 3DES with SHA test failed

Crypto MD5 test failed

VPN Client Policy Provisioning

IKE Initiator: Accepting IPSec proposal (Phase 2)

IKE Responder: Aggressive Mode complete (Phase 1)

Error initializing Hardware acceleration for VPN

PPTP Control Connection Negotiation Started
PPTP Session Negotiation Started
PPTP Max Retransmission Exceeded
PPTP Control Connection Established
PPTP Tunnel Disconnect from Remote
PPTP Session Established
PPTP Session Disconnect from Remote
PPTP PPP Negotiation Started
PPTP LCP Down
PPTP PPP Session Up
PPTP PPP Down
PPTP PPP Authentication Failed
PPTP LCP Up
PPTP Disconnect Initiated by the User
Disconnecting PPTP Tunnel due to traffic timeout
PPTP Connect Initiated by the User
PPTP PPP link down
PPTP starting CHAP Authentication
PPTP starting PAP Authentication
PPTP CHAP Authentication Failed. Please verify PPTP username and password
PPTP PAP Authentication Failed
PPTP PAP Authentication success.
PPTP PAP Authentication Failed. Please verify PPTP username and password
PPTP PPP Link Up
PPTP PPP Link down
PPTP PPP Link Finished
IKE Initiator: Received notify. NO_PROPOSAL_CHOSEN
IKE Responder: IKE proposal does not match (Phase 1)
IKE negotiation aborted due to timeout
Failed payload verification after decryption. Possible preshared key mismatch
Failed payload verification after decryption
Received packet retransmission. Drop duplicate packet
SA is disabled. Check VPN SA settings
Anti-Virus Licenses Exceeded
Received notify: ISAKMP_AUTH_FAILED
Computed hash does not match hash received from peer
Received notify: PAYLOAD_MALFORMED
Received IPSEC SA delete request
Received IKE SA delete request
Received notify: INVALID_COOKIES
Received notify: RESPONDER_LIFETIME
Received notify: INVALID_SPI
PKI Error:
IKE Responder: Proposed local network is 0.0.0.0 but SA has no LAN Default Gateway
RIP disabled on LAN interface
RIPv1 enabled on LAN interface
RIPv2 enabled on LAN interface
RIPv2 compatibility (broadcast) mode enabled on LAN interface

RIP disabled on DMZ interface

RIPv1 enabled on DMZ interface

RIPv2 enabled on DMZ interface

RIPv2 compatibility (broadcast) mode enabled on DMZ interface

IPSecTunnel status changed

Source routed IP packet dropped

No response from server to Echo Requests, disconnecting PPTP Tunnel

No response from PPTP server to control connection requests

No response from PPTP server to call requests

PPTP server rejected control connection

PPTP server rejected the call request

PPP Dial-Up: Trying to failover but Alternate Profile is manual

Failback initiated by %s

Probing succeeded on %s

E-Mail fragment dropped

Locked out user re-enabled - lockout period expired

Locked out user re-enabled by admin

Access Rule added

Access Rule modified

Access Rule deleted

Access Rules restored to defaults

PPTP Server is not responding, check if the server is UP and running.

IKE Initiator: Accepting peer lifetime. (Phase 1)

FTP: PASV response spoof attack dropped

PKI Failure

PKI Failure: Output buffer too small

PKI Failure: Cannot alloc memory

PKI Failure: Reached the limit for local certs, cant load any more

PKI Failure: Import failed

PKI Failure: Incorrect admin password

PKI Failure: CA certificates store does not have space to hold all the CA certificates required to verify this Local Certificate

PKI Failure: Improper file format. Please select PKCS#12 (*.p12) file

PKI Failure: Certificate's ID does not match this SonicWall

PKI Failure: public-private key mismatch

PKI Failure: Duplicate local certificate name

PKI Failure: Duplicate local certificate

PKI Failure: No CA certificates yet loaded

PKI Failure: Internal error

PKI Failure: Temporary memory shortage, try again

PKI Failure: The certificate chain is circular

PKI Failure: The certificate chain is incomplete

PKI Failure: The certificate chain has no root

PKI Failure: The certificate or a certificate in the chain has expired

PKI Failure: The certificate or a certificate in the chain has a validity period in the future

PKI Failure: The certificate or a certificate in the chain is corrupt

PKI Failure: The certificate or a certificate in the chain has a bad signature

PKI Failure: Loaded but could not verify certificate

PKI Failure: Loaded the certificate but could not verify it's chain

VPN Cleanup: Dynamic network settings change

WARNING: Central Gateway does not have a Relay IP Address. DHCP message dropped.

DHCP REQUEST received from remote device

DHCP DISCOVER received from remote device

DHCP DECLINE received from remote device

DHCP OFFER received from server

DHCP NAK received from server

ERROR: DHCP over VPN policy is not defined. Cannot start IKE.

DHCP DISCOVER received from local device

DHCP REQUEST received from local device

PPP Dial-Up: No peer IP address from Dial-Up ISP, local and remote IPs will be the same

Received AV Alert: Your SonicWALL Network Anti-Virus subscription will expire in 7 days. %s

Received notify: INVALID_ID_INFO

DHCP lease dropped. Lease from Central Gateway conflicts with Remote Management IP

SonicOS 1.0

SonicWALL activated

Log Cleared

Log successfully sent via email

Log full; deactivating SonicWALL

New URL List loaded

No new URL List available

Problem loading the URL List; check Filter settings

Problem loading the URL List; check your DNS server

Problem sending log email; check log settings

Restarting SonicWALL; dumping log to email

Web site blocked

Newsgroup blocked

Web site accessed

Newsgroup accessed

ActiveX blocked

Java blocked

ActiveX or Java archive blocked

Cookie removed

Ping of death blocked

IP spoof detected

Illegal LAN address in use

Possible SYN flood attack

Probable SYN flood attack

Land Attack Dropped

Fragmented Packet Dropped

Successful administrator login

Administrator login failed - incorrect password

Successful local user login

User login failed - incorrect password

Unknown user attempted to log in

Login screen timed out

Attempted administrator login from %s
TCP connection dropped
UDP packet dropped
ICMP packet dropped
PPTP packet dropped
IPSec packet dropped
Unknown protocol dropped
IPSec packet dropped; waiting for pending IPSec connection
IPSec connection interrupt
NAT could not remap incoming packet
ARP timeout
Broadcast packet dropped
No ICMP redirect sent
Out-of-order command packet dropped
Failure to add data channel
RealAudio decode failure
Duplicate packet dropped
No HOST tag found in HTTP request
The cache is full; %d open connections; some will be dropped
Code:
Type:
Source:
Destination:
License exceeded: Connection dropped because too many IP addresses are in use on your LAN
Rule
Access to Proxy Server Blocked
Diagnostic Code E
Dynamic IPSec client connected
Received fragmented packet or fragmentation needed
Diagnostic Code D
Illegal IPSec SPI
Unknown IPSec SPI
IPSec Authentication Failed
IPSec Decryption Failed
Incompatible IPSec Security Association
IPSec packet from or to an illegal host
SPI:
NetBus Attack Dropped
Back Orifice Attack Dropped
Net Spy Attack Dropped
Sub Seven Attack Dropped
Ripper Attack Dropped
Striker Attack Dropped
Senna Spy Attack Dropped
Priority Attack Dropped
Ini Killer Attack Dropped
Smurf Amplification Attack Dropped
Possible Port Scan

Probable Port Scan
Failed to resolve name
local range:
remote range:
IKE Responder: Accepting IPSec proposal (Phase 2)
IKE Responder: IPSec proposal does not match (Phase 2)
IKE negotiation complete. Adding IPSec SA. (Phase 2)
Starting IKE negotiation
Deleting IPSec SA for destination
Deleting IPSec SA
Diagnostic Code A
Diagnostic Code B
Diagnostic Code C
Status
#Web site hit
#Connection
Retransmitting DHCP DISCOVER.
Retransmitting DHCP REQUEST (Requesting).
Retransmitting DHCP REQUEST (Renewing).
Retransmitting DHCP REQUEST (Rebinding).
Retransmitting DHCP REQUEST (Rebooting).
Retransmitting DHCP REQUEST (Verifying).
Sending DHCP DISCOVER.
DHCP Server not available. Did not get any DHCP OFFER.
Got DHCP OFFER. Selecting.
Sending DHCP REQUEST.
DHCP Client did not get DHCP ACK.
DHCP Client got NACK.
DHCP Client got ACK from server.
DHCP Client is declining address offered by the server.
DHCP Client sending REQUEST and going to REBIND state.
DHCP Client sending REQUEST and going to RENEW state.
Sending DHCP REQUEST (Renewing).
Sending DHCP REQUEST (Rebinding).
Sending DHCP REQUEST (Rebooting).
Sending DHCP REQUEST (Verifying).
DHCP Client failed to verify and lease has expired. Go to INIT state.
DHCP Client failed to verify and lease is still valid. Go to BOUND state.
DHCP Client got a new IP address lease.
Sending DHCP RELEASE.
Access attempt from host without Anti-Virus agent installed
Anti-Virus agent out-of-date on host
Received AV Alert: %s
Unused AV log entry.
Starting PPPoE discovery
PPPoE LCP Link Up
PPPoE LCP Link Down
PPPoE terminated

PPPoE Network Connected
PPPoE Network Disconnected
PPPoE discovery process complete
PPPoE starting CHAP Authentication
PPPoE starting PAP Authentication
PPPoE CHAP Authentication Failed
PPPoE PAP Authentication Failed
Wan IP Changed
XAUTH Succeeded with VPN client
XAUTH Failed with VPN client, Authentication failure
XAUTH Failed with VPN client, Cannot Contact RADIUS Server
Log Debug
Add an attack message
Primary firewall has transitioned to Active
Backup firewall has transitioned to Active
Primary firewall has transitioned to Idle
Backup firewall has transitioned to Idle
Primary missed heartbeats from Active Backup: Primary going Active
Backup missed heartbeats from Active Primary: Backup going Active
Primary received error signal from Active Backup: Primary going Active
Backup received error signal from Active Primary: Backup going Active
Backup firewall being preempted by Primary
Primary firewall preempting Backup
Active Backup detects Active Primary: Backup going Idle
Imported HA hardware ID did not match this firewall
Discovered HA Backup Firewall
HA Peer Firewall Synchronized
Error Synchronizing HA Peer Firewall
Received AV Alert: Your SonicWALL Network Anti-Virus subscription has expired. %s
Primary received heartbeat from wrong source
Backup received heartbeat from wrong source
HA packet processing error
Heartbeat received from incompatible source
Diagnostic Code F
Forbidden E-Mail attachment disabled
PPPoE PAP Authentication success.
PPPoE PAP Authentication Failed. Please verify PPPoE username and password
Disconnecting PPPoE due to traffic timeout
No response from ISP Disconnecting PPPoE.
Backup going Active in preempt mode after reboot
VPN Log
VPN Log Debug
Denied TCP connection from LAN
Denied UDP packet from LAN
Denied ICMP packet from LAN
Firewall access from LAN
Probable TCP FIN scan
Probable TCP XMAS scan

Probable TCP NULL scan
IPSEC Replay Detected
TCP FIN packet dropped
Received a path MTU icmp message from router/gateway
Problem loading the URL List; Appliance not registered.
Problem loading the URL List; Subscription expired.
Problem loading the URL List; Try loading it again.
Problem loading the URL List; Retrying later.
Problem loading the URL List; Flash write failure.
Received a path MTU icmp message from router/gateway
MTU:
The loaded content URL List has expired.
Error setting the IP address of the backup, please manually set to backup LAN IP
Error updating HA peer configuration
Fraudulent Microsoft Certificate Blocked
VPN TCP SYN
VPN TCP FIN
VPN TCP PSH
Content filter subscription expired.
New firmware available.
Successful administrator login from the CLI
Administrator login failed - incorrect password from the CLI
L2TP Tunnel Negotiation Started
L2TP Session Negotiation Started
L2TP Max Retransmission Exceeded
L2TP Tunnel Established
L2TP Tunnel Disconnect from Remote
L2TP Session Established
L2TP Session Disconnect from Remote
L2TP PPP Negotiation Started
L2TP LCP Down
L2TP PPP Session Up
L2TP PPP Down
L2TP PPP Authentication Failed
L2TP LCP Up
L2TP Disconnect Initiated by the User
Disconnecting L2TP Tunnel due to traffic timeout
L2TP Connect Initiated by the User
L2TP PPP link down
Primary WAN link down, Primary going Idle
Backup WAN link down, Primary going Active
Primary WAN link down, Backup going Active
Primary WAN link up, preempting Backup
DHCP RELEASE relayed to Central Gateway
DHCP lease relayed to local device
DHCP RELEASE received from remote device
DHCP lease relayed to remote device
DHCP lease to LAN device conflicts with remote device, deleting remote IP entry

WARNING: DHCP lease relayed from Central Gateway conflicts with IP in Static Devices list

DHCP lease dropped. Lease from Central Gateway conflicts with Relay IP

IP spoof detected on packet to Central Gateway, packet dropped

Request for Relay IP Table from Central Gateway

Requesting Relay IP Table from Remote Gateway

Sent Relay IP Table to Central Gateway

Obtained Relay IP Table from Remote Gateway

Failed to synchronize Relay IP Table

Successful administrator login

Successful administrator login

Successful remote user login

Successful remote user login

NAT Discovery : Peer IPSec Security Gateway behind a NAT/NAPT Device

NAT Discovery : Local IPSec Security Gateway behind a NAT/NAPT Device

NAT Discovery : No NAT/NAPT device detected between IPSec Security gateways

NAT Discovery : Peer IPSec Security Gateway doesn't support VPN NAT Traversal

User login failed - RADIUS authentication failure

User login failed - RADIUS server timeout

User login failed - RADIUS configuration error

User login failed - User has no privileges for login from that location

IPSec packet from an illegal host

Forbidden E-Mail attachment deleted

IKE Responder: Mode %d - not tunnel mode

IKE Responder: No matching Phase 1 ID found for proposed remote network

IKE Responder: Proposed remote network is 0.0.0.0 but not DHCP relay nor default route

IKE Responder: No match for proposed remote network address

IKE Responder: Default LAN gateway is set but peer is not proposing to use this SA as a default route

IKE Responder: Tunnel terminates outside firewall but proposed local network is not NAT public address

IKE Responder: Tunnel terminates inside firewall but proposed local network is not inside firewall

IKE Responder: Tunnel terminates on DMZ but proposed local network is on LAN

IKE Responder: Tunnel terminates on LAN but proposed local network is on DMZ

IKE Responder: AH Perfect Forward Secrecy mismatch

IKE Responder: ESP Perfect Forward Secrecy mismatch

IKE Responder: Algorithms and/or keys do not match

Administrator logged out

Administrator logged out - inactivity timer expired

User logged out

User logged out - max session time exceeded

User logged out - inactivity timer expired

NAT device may not support IPSec AH passthrough

TCP Xmas Tree Blocked

CFL auto-download disabled, time problem detected

Requesting CRL from

CRL Loaded from

Failed to get CRL from

Not enough memory to hold the CRL

Connection timed out

Cant connect to the CRL server

Unknown reason
Failed to Process CRL from
Bad CRL format
Issuer match failed
Certificate on Revoked list(CRL)
No Certificate for
PPP Dial-Up: Dialing: %s
PPP Dial-Up: No dialtone detected - check phone-line connection
PPP Dial-Up: No link carrier detected - check phone number
PPP Dial-Up: Dialed number is busy
PPP Dial-Up: Dialed number did not answer
PPP Dial-Up: Connected at %s bps - starting PPP
PPP Dial-Up: Unknown dialing failure
PPP Dial-Up: Link carrier lost
PPP: Authentication successful
PPP: PAP Authentication failed - check username / password
PPP: CHAP authentication failed - check username / password
PPP: MS-CHAP authentication failed - check username / password
PPP: Starting MS-CHAP authentication
PPP: Starting CHAP authentication
PPP: Starting PAP authentication
PPP Dial-Up: PPP negotiation failed - disconnecting
PPP Dial-Up: Idle time limit exceeded - disconnecting
PPP Dial-Up: Failed to get IP address
PPP Dial-Up: Received new IP address
PPP Dial-Up: PPP link established
PPP Dial-Up: PPP link down
PPP Dial-Up: Shutting down link
PPP Dial-Up: Initialization : %s
PPP Dial-Up: User requested disconnect
PPP Dial-Up: User requested connect
PPP Dial-Up: Connect request canceled
The network connection in use is %s
L2TP Server : L2TP Tunnel Established.
L2TP Server : L2TP Session Established.
L2TP Server : L2TP PPP Session Established.
L2TP Server: Radius reports Authentication Failure
L2TP Server: Local Authentication Failure
L2TP Server: Radius server not assigned IP address
L2TP Server: No IP address available in the Local IP Pool
L2TP Server: L2TP Tunnel Disconnect from the Remote.
L2TP Server: L2TP Session Disconnect from the Remote.
L2TP Server: L2TP Remote terminated the PPP session
L2TP Server: Local Authentication Success.
L2TP Server: Radius Authentication Success
L2TP Server: Keep alive Failure. Closing Tunnel
PPP Dial-Up: Manual intervention needed. Check profile or disconnect or redial
PPP Dial-Up: Trying to failover but Primary Profile is manual

PPP Dial-Up: Startup without Ethernet cable, will try to dial on outbound traffic

PPP Dial-Up: Dial initiated by %s

The current WAN interface is not ready to route packets.

Probing failure on %s

PPP Dial-Up: Maximum connection time exceeded - disconnecting

Adminstrator name changed

User login failure rate exceeded - source address locked out

PPP Dial-Up: The profile in use disabled VPN networking.

PPP Dial-Up: VPN networking restored.

%s Ethernet Port Up

%s Ethernet Port Down

L2TP Server: Call Disconnect from Remote.

L2TP Server: Tunnel Disconnect from Remote.

L2TP Server : Deleting the Tunnel

L2TP Server : Deleting the L2TP active Session

L2TP Server : Retransmission Timeout, Deleting the Tunnel

NAT translated packet exceeds size limit, packet dropped

HTTP management port has changed

HTTPS management port has changed

IKE Responder: Mode %d - not transport mode. Xauth is required but not supported by peer.

L2TP Server : Access from L2TP VPN Client Privilege not enabled for Radius Users.

L2TP Server : User Name authentication Failure locally.

IKE Responder: Tunnel terminates outside firewall but proposed remote network is not NAT public address

IKE Initiator: Start Quick Mode (Phase 2).

Port configured to receive IPSEC ONLY. Drop packet received in the clear.

Imported VPN SA is invalid - disabled

IPSEC SA lifetime expired.

IKE SA lifetime expired.

IKE Initiator: Start Main Mode negotiation (Phase 1)

IKE Responder: Received Quick Mode Request (Phase 2)

IKE Initiator: Main Mode complete (Phase 1)

IKE Initiator: Aggressive Mode complete (Phase 1).

IKE Responder: Received Main Mode request (Phase 1)

IKE Responder: Received Aggressive Mode request (Phase 1)

IKE Responder: Main Mode complete (Phase 1)

IKE Initiator: Start Aggressive Mode negotiation (Phase 1)

Entering FIPS ERROR state

Crypto DES test failed

Crypto DH test failed

Crypto Hmac-MD5 fest failed

Crypto Hmac-Sha1 test failed

Crypto RSA test failed

Crypto Sha1 test failed

Crypto hardware DES test failed

Crypto Hardware 3Des test failed

Crypto Haredware DES with SHA test failed

Crypto Hardware 3DES with SHA test failed

Crypto MD5 test failed

VPN Client Policy Provisioning
IKE Initiator: Accepting IPSec proposal (Phase 2)
IKE Responder: Aggressive Mode complete (Phase 1)
Error initializing Hardware acceleration for VPN
PPTP Control Connection Negotiation Started
PPTP Session Negotiation Started
PPTP Max Retransmission Exceeded
PPTP Control Connection Established
PPTP Tunnel Disconnect from Remote
PPTP Session Established
PPTP Session Disconnect from Remote
PPTP PPP Negotiation Started
PPTP LCP Down
PPTP PPP Session Up
PPTP PPP Down
PPTP PPP Authentication Failed
PPTP LCP Up
PPTP Disconnect Initiated by the User
Disconnecting PPTP Tunnel due to traffic timeout
PPTP Connect Initiated by the User
PPTP PPP link down
PPTP starting CHAP Authentication
PPTP starting PAP Authentication
PPTP CHAP Authentication Failed. Please verify PPTP username and password
PPTP PAP Authentication Failed
PPTP PAP Authentication success.
PPTP PAP Authentication Failed. Please verify PPTP username and password
PPTP PPP Link Up
PPTP PPP Link down
PPTP PPP Link Finished
IKE Initiator: Received notify. NO_PROPOSAL_CHOSEN
IKE Responder: IKE proposal does not match (Phase 1)
IKE negotiation aborted due to timeout
Failed payload verification after decryption. Possible preshared key mismatch
Failed payload verification after decryption
Received packet retransmission. Drop duplicate packet
SA is disabled. Check VPN SA settings
Anti-Virus Licenses Exceeded
Received notify: ISAKMP_AUTH_FAILED
Computed hash does not match hash received from peer
Received notify: PAYLOAD_MALFORMED
Received IPSEC SA delete request
Received IKE SA delete request
Received notify: INVALID_COOKIES
Received notify: RESPONDER_LIFETIME
Received notify: INVALID_SPI
PKI Error:
IKE Responder: Proposed local network is 0.0.0.0 but SA has no LAN Default Gateway

RIP disabled on LAN interface
RIPv1 enabled on LAN interface
RIPv2 enabled on LAN interface
RIPv2 compatibility (broadcast) mode enabled on LAN interface
RIP disabled on DMZ interface
RIPv1 enabled on DMZ interface
RIPv2 enabled on DMZ interface
RIPv2 compatibility (broadcast) mode enabled on DMZ interface
IPSecTunnel status changed
Source routed IP packet dropped
No response from server to Echo Requests, disconnecting PPTP Tunnel
No response from PPTP server to control connection requests
No response from PPTP server to call requests
PPTP server rejected control connection
PPTP server rejected the call request
PPP Dial-Up: Trying to failover but Alternate Profile is manual
Failback initiated by %s
Probing succeeded on %s
E-Mail fragment dropped
Locked out user re-enabled - lockout period expired
Locked out user re-enabled by admin
Access Rule added
Access Rule modified
Access Rule deleted
Access Rules restored to defaults
PPTP Server is not responding, check if the server is UP and running.
IKE Initiator: Accepting peer lifetime. (Phase 1)
FTP: PASV response spoof attack dropped
PKI Failure
PKI Failure: Output buffer too small
PKI Failure: Cannot alloc memory
PKI Failure: Reached the limit for local certs, cant load any more
PKI Failure: Import failed
PKI Failure: Incorrect admin password
PKI Failure: CA certificates store does not have space to hold all the CA certificates required to verify this Local Certificate
PKI Failure: Improper file format. Please select PKCS#12 (*.p12) file
PKI Failure: Certificate's ID does not match this SonicWall
PKI Failure: public-private key mismatch
PKI Failure: Duplicate local certificate name
PKI Failure: Duplicate local certificate
PKI Failure: No CA certificates yet loaded
PKI Failure: Internal error
PKI Failure: Temporary memory shortage, try again
PKI Failure: The certificate chain is circular
PKI Failure: The certificate chain is incomplete
PKI Failure: The certificate chain has no root
PKI Failure: The certificate or a certificate in the chain has expired
PKI Failure: The certificate or a certificate in the chain has a validity period in the future

PKI Failure: The certificate or a certificate in the chain is corrupt

PKI Failure: The certificate or a certificate in the chain has a bad signature

PKI Failure: Loaded but could not verify certificate

PKI Failure: Loaded the certificate but could not verify it's chain

VPN Cleanup: Dynamic network settings change

WARNING: Central Gateway does not have a Relay IP Address. DHCP message dropped.

DHCP REQUEST received from remote device

DHCP DISCOVER received from remote device

DHCP DECLINE received from remote device

DHCP OFFER received from server

DHCP NAK received from server

ERROR: DHCP over VPN policy is not defined. Cannot start IKE.

DHCP DISCOVER received from local device

DHCP REQUEST received from local device

PPP Dial-Up: No peer IP address from Dial-Up ISP, local and remote IPs will be the same

Received AV Alert: Your SonicWALL Network Anti-Virus subscription will expire in 7 days. %s

Received notify: INVALID_ID_INFO

DHCP lease dropped. Lease from Central Gateway conflicts with Remote Management IP

Category:

User login failed - User has no privileges for wlan guest service

wlan firmware image has been updated

Packet dropped by wlan guest check

Received CFS Alert: Your SonicWALL Content Filtering subscription will expire in 7 days.

Received CFS Alert: Your SonicWALL Content Filtering subscription has expired.

Received E-Mail Filter Alert: Your SonicWALL E-Mail Filtering subscription will expire in 7 days.

Received E-Mail Filter Alert: Your SonicWALL E-Mail Filtering subscription has expired.

ISDN Driver Firmware successfully updated

Global VPN Client License Exceeded: Connection denied.

Packet dropped by wlan vpn traversal check

SonicWALL Registration Update Needed: Restore your existing security service subscriptions by clicking here.

Entering FIPS Error State.

WAN Interface not setup

PPPoE enabled but not ready

L2TP enabled but not ready

PPTP enabled but not ready

WAN not ready

VPN disabled for active dial up

DHCP client enabled but not ready

Blocked Quick Mode for Client using Default KeyId

VPN disabled by administrator

VPN enabled by administrator

WLAN disabled by administrator

WLAN enabled by administrator

WiFiSec Enforcement disabled by administrator

WiFiSec Enforcement enabled by administrator

Wireless MAC Filter List enabled by administrator

Wireless MAC Filter List disabled by administrator

PPPoE user name changed by Administrator

PPPoE password changed by Administrator

IKE Responder: Default LAN gateway is not set but peer is proposing to use this SA as a default route

Diagnostic Code D

802.11b Management

wlan recovery

Administrator logged out from the CLI

SonicWALL initializing

Malformed IP packet dropped.

ICMP packet dropped

Web access request dropped

Protocol:

Web access request received

FTP: PORT bounce attack dropped.

FTP: PASV response bounce attack dropped.

Global VPN Client connection is not allowed. Appliance is not registered.